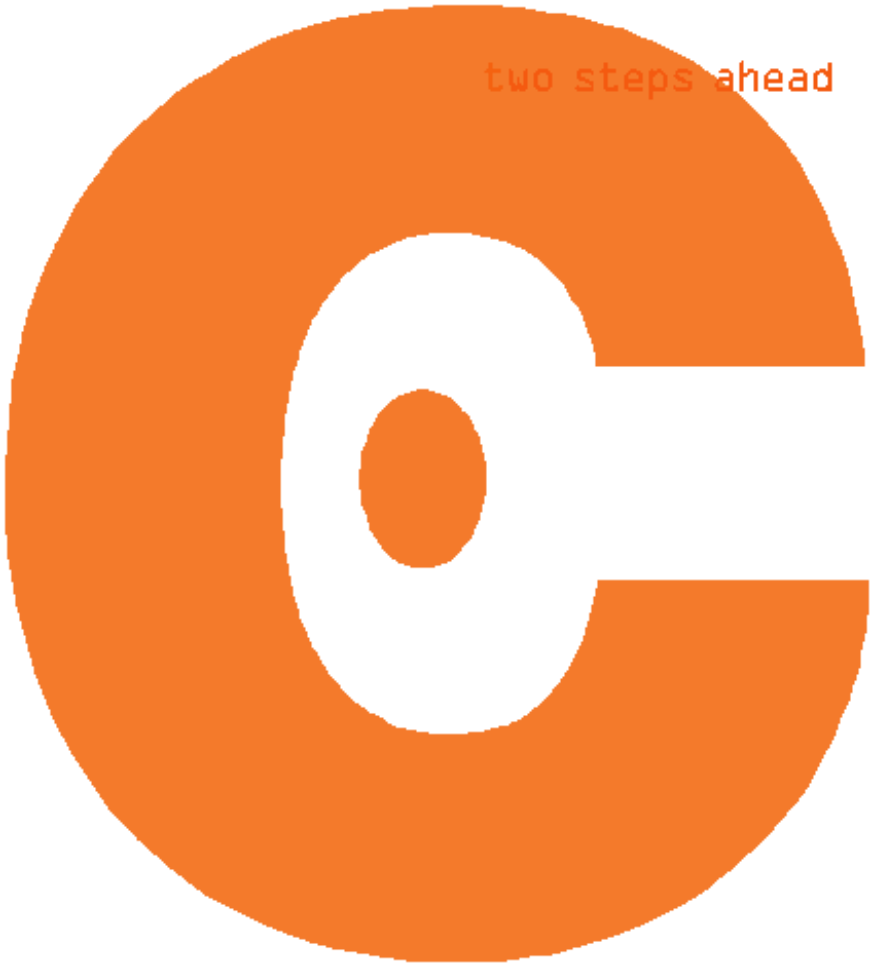


HOTSIGN

Benutzerhandbuch

Version 1.0.8
Datum 23.09.2014
Autor Markus Punz

© BDC EDV-Consulting GmbH office@bdc.at http://www.bdc.at

1. Inhaltsverzeichnis

1. Inhaltsverzeichnis 2
2. Über dieses Dokument 3
2.1. Zweck 3
3. Überblick 3
4. Systemvoraussetzungen 4
5. Editionen von hotSign 5
6. Hinweise 5
6.1. Sicherheitshinweise 5
6.2. Disclaimer 5
6.3. Benutzerhinweise 6
7. Installation 6
7.1. Allgemein 6
7.2. Erstinstallation 6
7.2.1. Produktaktivierung 10
7.2.2 *Installation der Zusatzsoftware* 13
7.2.2.1 hotPDFVerify für Adobe Reader 13
7.3. Änderung von Kartenlesegerät und/oder Port 13
7.4. Grundsätzliches zur Kartenlesegeräten und Interfaces 14
7.5. Deinstallation 14
8. Allgemeine Informationen zur Bürgerkartenumgebung 16
8.1. Grundlagen zur Signatur und Zertifikaten 16
8.2. Die Bürgerkarte 16
8.3. Infoboxen der Bürgerkarte 17
8.3.1. Infobox für Zertifikate 17
8.3.2. Infobox für die Personenbindung 17
8.3.3. Infobox für Vollmachten 17
8.4. Formate der signierten Daten 17
8.5. Security-Layer 17
8.6. Ablaufbeispiel 18
8.7. Bürgerkarte FAQ 19
9. Programmbeschreibung 19
9.1. Programmstart/Beenden 19
9.1. Hash Verfahren auswählen 20
9.2. Erstellen einer Signatur 20
9.2.1. Durchführung 21
9.2.2. Mögliche Fehlerursachen 24
9.3. Signaturverifikation 24
9.3.1. Durchführung 25
9.3.2. Mögliche Fehlerursachen 27
9.4. hotSign Module 28
9.4.1. PIN ändern 28
9.4.2. PIN aktivieren 31
9.4.3. PIN entsperren 33
9.4.4. Beliebige Datei signieren/verifizieren 35
9.4.5. Infoboxen anzeigen 41
10. Verwaltungsfunktionen 43
10.1. Zertifizierungsinstanzen 43
10.1.1. Zertifizierungsinstanz hinzufügen 44
10.1.2. Daten einer Zertifizierungsinstanz ändern 44

10.1.3. Zertifizierungsinstanz löschen 45
10.2. Zertifikatsverwaltung 45
10.2.1. Übersicht 45
10.2.2. Hinzufügen eines Zertifikats 46
10.2.3. Löschen eines Zertifikats 47
10.3. Proxy-Einstellungen 47
10.4. PDF Konfiguration 48
10.5. hotSign Aktivierung 48
10.6. Weitere Funktionen 49
10.6.1. Protokoll aufzeichnen 49
10.6.2. Autoupdate 49
10.6.3. Tip des Tages 49
10.6.4. Standard Infobox-PIN verwenden 50
10.6.5. Über BDC "hotSign" 50
11. Barrierefreiheit 50
12. Häufige Fehlerursachen 50
13. hotSign FAQ 51
13.1. Installation 51
13.2. Betrieb 51
14. Glossar 52
15. Benutzte Bibliotheken 53
16. Lizenzen 53
16.1. CDSA 53
16.2. VXCL 54
16.3. OpenSSL 55
16.4. Apache Software Foundation 58

2. Über dieses Dokument

2.1. Zweck

Dieses Dokument ist das Benutzerhandbuch der "**hotSign** 2.0.0" Bürgerkartenumgebung und beschreibt die Installation, Bedienelemente sowie die Sicherheitsmaßnahmen. Die Herausgeber behalten sich vor, die beschriebenen Schnittstellen und Abläufe nötigenfalls zu ändern.

3. Überblick

Die Bürgerkartenumgebung **hotSign** wurde speziell für die Erstellung von elektr. Signaturen im E-Government Bereich entwickelt.
hotSign erfüllt alle Auflagen des österreichischen Signaturgesetzes bezüglich des Erstellens qualifizierter Signaturen und ist kompatibel zum Security-Layer-Protokoll für das Konzept Bürgerkarte in der Version 1.2.

Die Bürgerkartenumgebung **hotSign** kapselt die für den Support von PKI (Public Key Infrastructure) erforderlichen Funktionalitäten und stellt PKI–Funktionen über eine definierte, einfach zu implementierende und leistungsfähige Schnittstelle zur Verfügung.
Die Bürgerkartenumgebung **hotSign** ist in der Lage, sowohl qualifizierte wie auch einfache elektronische Signaturen (nach Ö–SigG) zu erstellen, und diese auch zu verifizieren. Zudem enthält **hotSign** Funktionen, die für die Identifikation im Rahmen von E-Government Applikationen zwingend erforderlich sind (Personenbindung).

hotSign stellt außerdem Programmmodule zum:

- Ändern der Signatur–PIN
- Entsperren einer PIN
- Signieren/Verifizieren von beliebigen Dateien
- Infoboxen auslesen
- Verwaltung von Zertifizierungsinstanzen
- Verwaltung von vertrauenswürdigen Zertifikaten
- Verwaltung von Proxy-Einstellungen sowie
- Autoupdate durchführen
- Anzeigen des „Tip des Tages“
- Aktivierung

zur Verfügung.

4. Systemvoraussetzungen

hotSign unterstützt die folgenden Versionen des Microsoft (TM) Windows Betriebssystems:

- ❑ Windows 2000 professional, **Service Pack 4+, Internet Explorer 6.0**
- ❑ Windows XP Home / Professional, **Service Pack 2+, Internet Explorer 6.0+**
- ❑ Windows Vista Home Basic / Home Premium / Business / Enterprise / Ultimate, **Internet Explorer 7.0+**
- ❑ Windows 7 (alle Editionen)
- ❑ Windows 8 / 8.1 (alle Editionen)

- Hardware (Mindestvoraussetzungen): siehe Mindestanforderungen des entsprechenden Betriebssystems
- Freigegebene Bildschirmauflösungen: 800 x 600 oder höher

Hinweis: *Eine Desktop–Farbtiefe von mind. 24 Bit (16 Mio Farben) ist empfehlenswert. Diese ist erforderlich, falls auch Bilder (GIF bzw. JPEG) in die Anzeige und Signatur eingebunden werden. Ohne diese Voraussetzung ist eine Anzeige von Bildinformationen nicht möglich.*

Wir empfehlen folgende Kartenleser, die explizit mit **hotSign** getestet sind:

- KOBIL KAAN Professional
- KOBIL KAAN Advanced
- KOBIL EMV TriCAP
- REINER SCT cyberJack e-com
- REINER SCT cyberJack Secoder
- REINER SCT cyberJack KB
- REINER SCT cyberJack pinpad
- SCM SPR532
- Cherry Smartboards (G83-6700LQZ, G81-8015LQZ, G83-6744LBZ, G83-6744LUZ)
- Omnikey Cardman 3621
- Omnikey Cardman 3821

Weiters werden die folgenden **Signaturkarten** unterstützt:

- a.sign Premium Signaturkarte
- A-Trust eBilling Signaturkarte
- Österreichische Maestro-Karte mit Signaturfunktion
- eCard (**Achtung:** nur falls der e-Card Modul aktiviert ist)
- D-Trust card und D-Trust multicard (**Achtung:** nur falls der D-Trust Modul aktiviert ist)

hotSign mit Unterstützung der A-Trust Signaturkarten kann kostenlos von BDC bezogen werden. Weiters gibt es eine eCard-Edition von hotSign, die zusätzlich die eCard als Signaturkarte unterstützt. Die D-Trust Edition unterstützt die D-Trust Signaturkarten (D-Trust card und D-Trust multicard). Die kostenpflichtigen Module von hotSign können beliebig kombiniert werden. Ein Aktivierungscode kann über den Online-Shop von BDC bezogen werden.

5. Editionen von hotSign

hotSign als vollständige Bürgerkartenumgebung mit der Unterstützung der A-Trust Signaturkarten steht kostenlos zur Verfügung. Die Module:

- E-Card
- PDF-Signatur
- D-Trust

können zusätzlich erworben werden. Gesteuert wird dies über einen Aktivierungscode, der über den Online-Shop von BDC angefordert werden kann. Nach Erhalt des Aktivierungscodes muss dieser im Dialogfenster zusammen mit den Stammdaten des Benutzers eingegeben werden (siehe 10.5 hotSign Aktivierung).

6. Hinweise

6.1. Sicherheitshinweise

Die Installation von hotSign muss als Systemadministrator oder einem Benutzer mit Administratorrechten vorgenommen werden. Dies betrifft jedoch ausschließlich die Installation. Den Betrieb von hotSign empfehlen wir unbedingt mit einem Benutzer, der keine Administratorrechte am System besitzt. Wird hotSign unter einem Benutzer betrieben, der Schreibrechte in die Windows-Systemordner besitzt, kann die Integrität der hotSign Programmkomponenten nicht gewährleistet werden.

Während der Erstellung einer qualifizierten Signatur und während des Benutzens der Verwaltungsfunktionen darf der benutzte Computer nicht ferngewartet (zB durch die Fernwartungsfunktion von Windows ™) werden. In diesem Fall schließt der Hersteller von **hotSign** die fehlerfreie Erstellung einer qualifizierten Signatur und die Geheimhaltung des zu signierenden Dokuments, der PINs und der PUKs aus.

6.2. Disclaimer

BDC als Hersteller der Bürgerkartenumgebung **hotSign 2.0.0** schließt die fehlerfreie Erstellung einer qualifizierten Signatur nach dem österreichischen Signaturgesetz aus, wenn das benutzte Betriebsystem durch Viren oder Ähnliches verseucht ist.

Der Benutzer hat darauf zu achten, dass auf dem benutzten Computer eine regelmäßig aktualisierte Version eines gängigen Virenscanner installiert ist und regelmäßig verwendet wird. Außerdem hat der Benutzer darauf zu achten, dass nur solche Kartenlesegeräte verwendet werden, deren Sicherheitsmerkmale nicht verändert wurden. Falls nicht die originalen Lesegerätetreiber installiert sind, kann die Erstellung einer qualifizierten Signatur nicht garantiert werden.
Weiters wird eine Aufdeckung der Signatur–PIN nur dann ausgeschlossen, wenn keine anderen als die genannten unterstützten Kartenlesegeräte zum Erstellen der Signatur und zum Management der Signatur–Karte verwendet werden.

6.3. Benutzerhinweise

Bei Verwendung von Microsoft Windows Betriebssystemen ist es möglich, dass Viren oder andere bösartige Programme den dargestellten Inhalt eines Fensters verändern können. Die BDC **hotSign** Bürgerkartenumgebung verfügt über entsprechende Mechanismen, um solche Angriffe zu erkennen und abzuwehren. Um einen entsprechenden Angriff auf den Secure-Viewer zu verhindern, wird der dargestellte Inhalt in periodischen Abständen neu gezeichnet. Liegt ein Angriff durch einen Virus oder ein anderes bösartiges Programm vor, führt dies zum Flimmern des Secure-Viewers. Der Hersteller von **hotSign** weist darauf hin, dass keine Signatur erstellt werden darf, wenn der Secure-Viewer flimmert.
Der Hersteller von **hotSign** weist außerdem darauf hin, dass eine Eingabe der Signatur-PIN am PIN–Pad des Kartenlesegeräts, die Erstellung einer Signatur zur Folge hat. Der Benutzer muss sich im Klaren sein, dass die Eingabe der Signatur-PIN das Erstellen einer Signatur auslöst.
Bei Anzeige von Bilddaten im Secure-Viewer ist eine Desktopfarbtiefe von mindestens 24bit (16 Mio. Farben) erforderlich um mögliche Dithering–Effekte zu verhindern. Der Hersteller von **hotSign** weist darauf hin, dass daher für die Erstellung von qualifizierten Signaturen eine Desktopfarbtiefe von 24bit zwingend erforderlich ist. (Werden keine Bilddaten angezeigt, muss eine Desktopfarbtiefe von mindestens 8bit (256 Farben) gewährleistet sein)

7. Installation

7.1. Allgemein

Achtung: Für die Installation von **hotSign** sind Administratorrechte erforderlich. Unmittelbar nach der Installation empfehlen wir unbedingt eine Anmeldung mit Benutzerrechten. Die Integrität der **hotSign** Programmkomponenten kann ansonsten nicht gewährleistet werden.

Es ist ratsam, vor der Installation von **hotSign** den gewünschten **Kartenleser** sowie die entsprechenden Treiber zu **installieren.** Die Installationsroutine von **hotSign** scannt automatisch nach installierten Kartenlesegeräten.
Achten Sie darauf, dass Sie den **richtigen Kartenlesertreiber** verwenden (Empfehlungsliste der A-Trust). Stellen Sie sicher, dass der Kartenlesertreiber von einer **vertrauenswürdigen Quelle** stammt. Vergewissern Sie sich auch, dass eventuell **erforderliche Systemupdates** (siehe Kapitel 4 Systemvoraussetzungen) bereits durchgeführt wurden.

hotSign wird für ein bestimmtes Kartenlesegerät konfiguriert – das parallele Ansprechen von mehreren Kartenlesegeräten ist nicht möglich, jedoch können mehrere Kartenlesegeräte gleichzeitig auf dem verwendeten System installiert sein.

7.2. Erstinstallation

Nach dem Ausführen des Installationsprogrammes wird folgende Information angezeigt:

Figure 1: hotSign – Setup initialisieren

Danach wird die Auswahl des Installationsverzeichnisses ermöglicht:

Figure 2: hotSign – Auswahl Installationsverzeichnis

Bestätigen Sie durch markieren beider Hinweise, daß der Kartenleser bereits installiert und angeschlossen ist. Falls dies nicht zutrifft, beenden Sie das Setupprogramm und installieren Sie, vor neuerlicher Ausführung des Setup-Programmes, die entsprechenden Kartenlesegerätetreiber.

Figure 3: hotSign – Checkliste

Als nächsten Schritt versucht das **hotSign** Setup-Programm installierte Kartenleser aufzufinden:

Figure 4: hotSign – Suche nach Kartenlesegerät

Alle gefundenen Kartenleser werden in einer Liste angezeigt:

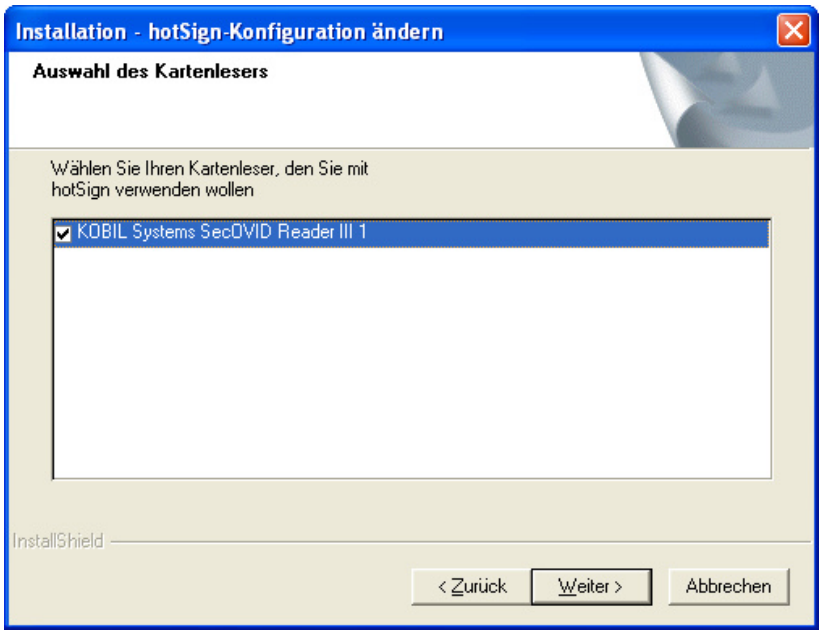


Figure 5: hotSign –Kartenleser, die im System vorhanden sind

Werden mehrere Kartenleser im System gefunden, muss der gewünschte Kartenleser ausgewählt werden (= Häkchen vor dem gewünschten Eintrag).

Konnte kein Kartenlesegerät gefunden werden, beantwortet dies **hotSign** mit einer entsprechenden Information:

Figure 6: hotSign – Setup-Fehlermeldung

Wenn Sie „Nein“ auswählen, wird die Installation abgebrochen. Bei „Ja“ werden alle Programmdateien von **hotSign** installiert, es wird allerdings kein Kartenlesegerät konfiguriert.
Die Kartenleser-Konfiguration kann in der Folge jederzeit über einen entsprechenden Programm-Menü Eintrag von **hotSign** gestartet werden.

In der Folge werden die Programmdateien in das zuvor gewählte Verzeichnis kopiert.
Nach dem Kopiervorgang werden noch Stammzertifikate in den vertrauenswürdigen Stammzertifikatsspeicher von Microsoft Windows eingetragen. Das erste Zertifikat trägt den Namen „localhost“ und ist für den ordnungsgemäßen Betrieb einiger eGovernment-Applikationen erforderlich. Wir empfehlen daher die Sicherheitsabfrage zu bestätigen.
Im gleichen Zusammenhang wird ebenfalls geprüft ob neue Stammzertifikate von A-Trust verfügbar sind, die in Ihrer Windows-Installation noch nicht eingetragen sind. Auch hier werden Sie aufgefordert den Import zu bestätigen.

Hinweis: Die A-Trust Stammzertifikate sind für die integrierte Updatefunktion von **hotSign** erforderlich. Diese ist in der Lage, aktuelle Versionen automatisch vom Update – Server herunterzuladen und zu installieren. Aus Sicherheitsgründen erfolgt dies mittels einer verschlüsselten Verbindung. Die nötigen SSL – Zertifikate werden vom Server des Zertifizierungsdiensteanbieter geladen und installiert.

*Hinweis zur Verwendung von **Proxys**: Soll die Internetverbindung unter Verwendung eines Proxy – Servers erfolgen, so verwendet **hotSign** die Windows – Systemeinstellungen. Diese befinden sich in der Windows - Systemsteuerung unter Punkt „Internetoptionen → Verbindungen → Einstellungen”. Hier finden Sie die Angaben zu den Proxy–Einstellungen des Systems. Sind diese Einstellungen nicht korrekt, wenden Sie sich an ihren Netzwerkadministrator bzw. an ihren Internetanbieter.*

Nach erfolgreichem Kopiervorgang der Programmdateien ins gewählte Installationsverzeichnis und nach erfolgter Konfiguration von **hotSign** ist das Setup abgeschlossen.

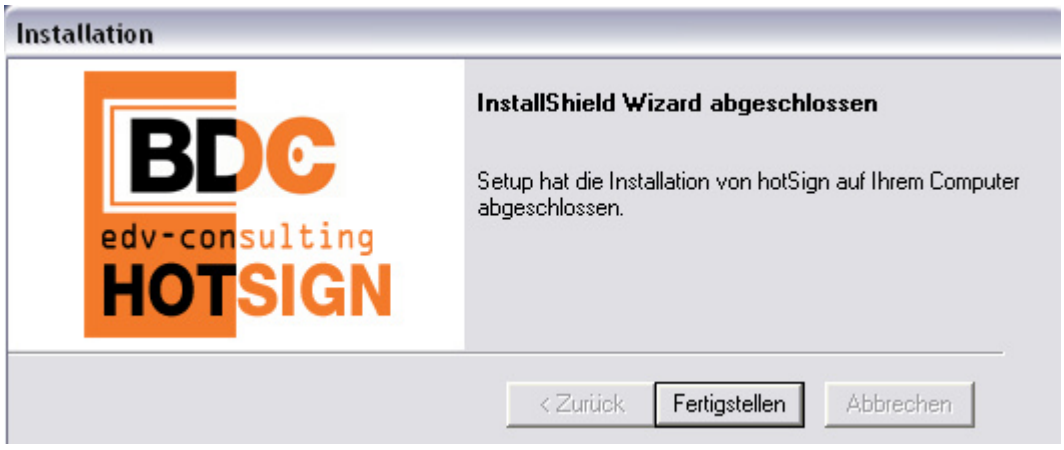


Figure 7: hotSign – Setup erfolgreich abgeschlossen

7.2.1. Produktaktivierung

Nachdem das Setup durch klicken auf die Schaltfläche „Fertigstellen“ abgeschlossen wurde, wird ein Dialog anzeigt, der die Möglichkeit bietet die kostenpflichtigen Features von **hotSign** zu aktivieren. Sie können wählen, ob Sie die Produktaktivierung sofort oder zu einem späteren Zeitpunkt über das **hotSign**-Kontextmenü vornehmen möchten. Ohne Aktivierung können die kostenpflichtigen Features (Unterstützung der eCard, Qualifizierte Signatur von PDF-Dokumenten, Unterstützung der D-Trust Signaturkarte) für einen Testzeitraum von 30 Tagen kostenlos verwendet werden. Nach Ablauf des Testzeitraums werden diese Features wieder deaktiviert. Die vollständige Bürgerkartenfunktionalität inkl. Unterstützung der A-Trust Signaturkarten steht auch nach Ablauf des Testzeitraums und ohne Produktaktivierung weiterhin kostenlos zur Verfügung.

Hinweis: Wurde auf Ihrem System bereits eine Produktaktivierung erfolgreich vorgenommen, wird dieser Dialog nicht mehr bei einer erneuten Installation von **hotSign** angezeigt.

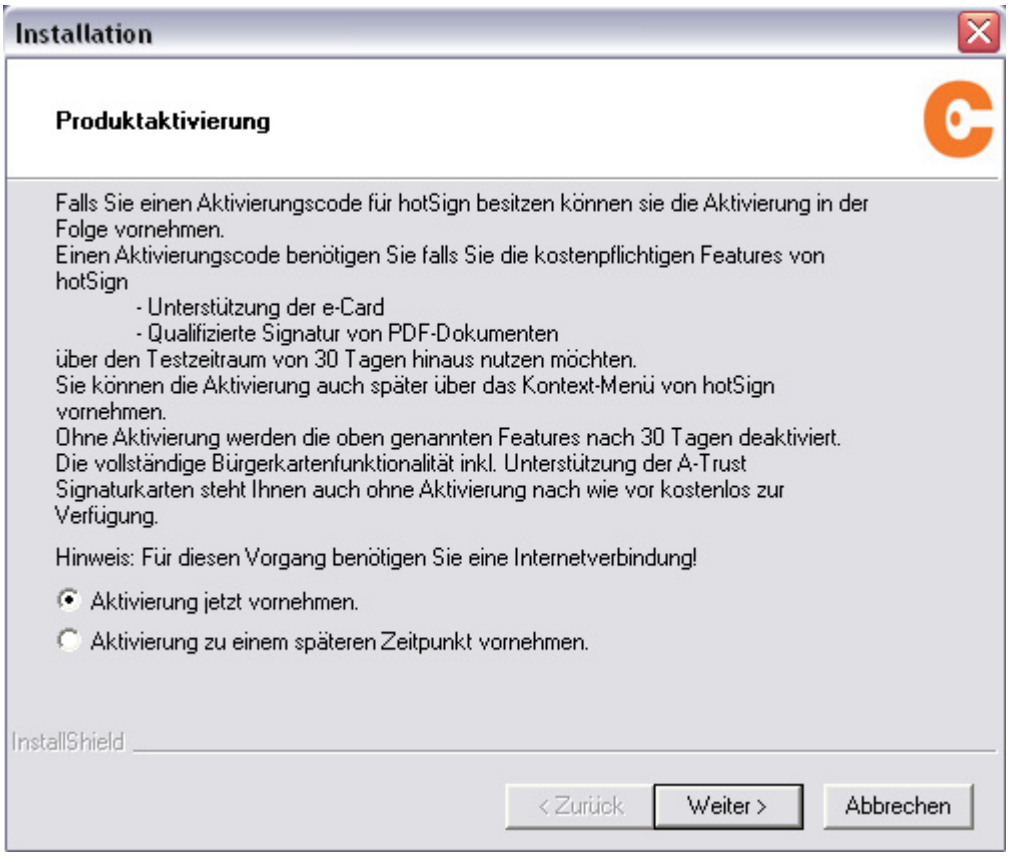


Figure 8: hotSign – Produktaktivierung

Wenn Sie „Aktivierung zu einem späteren Zeitpunkt vornehmen“ auswählen, wird der Aktivierungsvorgang beendet. Bei Auswahl von „Aktivierung jetzt vornehmen“ wird im nächsten Schritt ein Dialog angezeigt, der Sie zur Eingabe der erforderlichen Aktivierungsinformationen auffordert.

Achtung: Wenn Sie auf die Schaltfläche „Abbrechen“ klicken und den anschließenden Hinweis bestätigen, wird die Installation von **hotSign** nicht vollständig abgeschlossen und **hotSign** kann nicht verwendet werden.

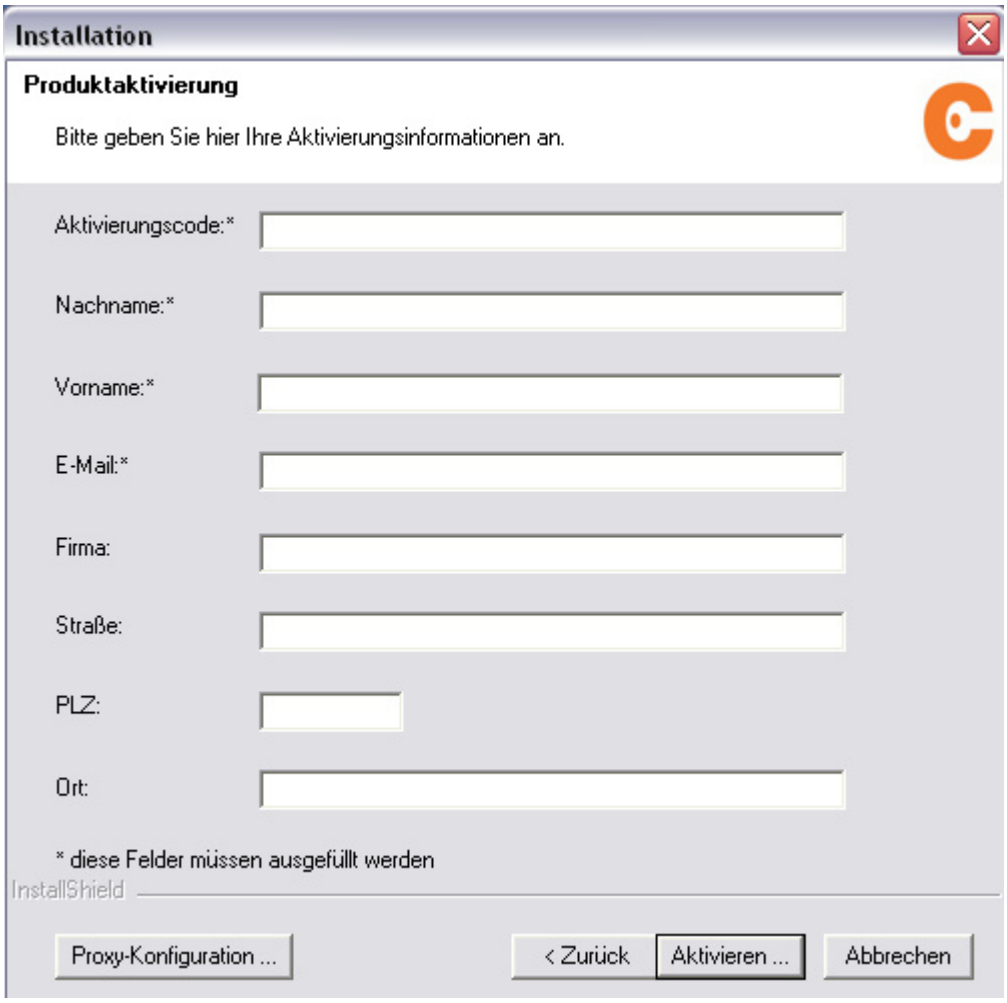


Figure 9: Eingabe der Aktivierungsinformationen

Werden nicht alle erforderlichen Felder ausgefüllt oder weist die E-Mail Adresse ein ungültiges Format auf, werden Sie mit einer entsprechenden Fehlermeldung darauf hingewiesen:

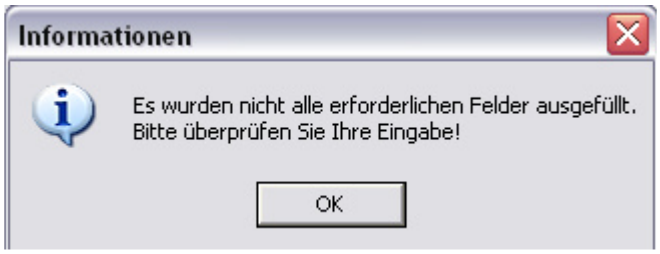


Figure 10: Fehlende Aktivierungsinformation(en)

Figure 11: Ungültige E-Mail Adresse

Für die Produktaktivierung müssen Sie über eine Internetverbindung verfügen. Erhalten Sie Zugang zum Internet über einen Proxy-Server, kann dieser über „Proxy-Konfiguration …“ eingetragen werden.

Figure 12: HTTPS Proxy-Server Konfiguration

Beim Klicken der Schaltfläche „Aktivieren …“ wird versucht eine Verbindung zum BDC Aktivierungsserver herzustellen und **hotSign** zu aktivieren. Je nach Geschwindigkeit Ihrer Internetverbindung kann diese einige Zeit in Anspruch nehmen:

Figure 13: Produktaktivierung wird durchgeführt

Konnte dieser Vorgang erfolgreich abgeschlossen werden, wird eine entsprechende Meldung angezeigt, ansonsten erhalten Sie einen Hinweis, warum die Produktaktivierung fehlgeschlagen ist.

Figure 14: Erfolgreiche Produktaktivierung

7.2.2 *Installation der Zusatzsoftware*

Nach Ende der Produktaktivierung haben Sie die Möglichkeit das Adobe Plugin **hotPDFVerify** von BDC zu installieren. Dieses Produkt ist kostenlos und dient Ihnen als Unterstützung bei der Signatur von PDF-Dokumenten. Es ist jedoch nicht für zwingend für die Verwendung von **hotSign** erforderlich.

7.2.2.1 hotPDFVerify für Adobe Reader

hotPDFVerify für Adobe Reader von BDC ist ein Adobe Reader Plugin, das dazu verwendet werden kann PDF-Dokumente, die im Adobe Reader geöffnet sind, auf dynamische Inhalte zu untersuchen. Wenn Sie **hotPDFVerify** installieren möchten, wählen Sie „Installieren…“ und der Installationsassistent von **hotPDFVerify** wird gestartet.

Hinweis: Für eine erfolgreiche Installation von **hotPDFVerify** muss ein Adobe Reader ab der Version 8.0 auf Ihrem System installiert sein.

Figure 20: Installation von hotPDFVerify

7.3. *Änderung von Kartenlesegerät und/oder Port*

Für den Fall, dass das bisher verwendete Kartenlesegerät durch ein Gerät anderen Typs ersetzt oder das vorhandene Lesegerät an einer anderen Schnittstelle angeschlossen wurde, ist wie folgt vorzugehen:

1. Bei Verwendung eines neuen Kartenlesegeräts - Installation der Lesertreiber, welche mit dem neuen Lesegerät geliefert werden.
2. Beenden von **hotSign**
3. Ausführen des **hotSign** Installationsprogrammes, oder Aufruf des Setups mit Hilfe der Softwareumgebung von Windows (**hotSign** in der Liste der bereits installierten Software auswählen)
4. „**hotSign** -Konfiguration ändern“ auswählen:

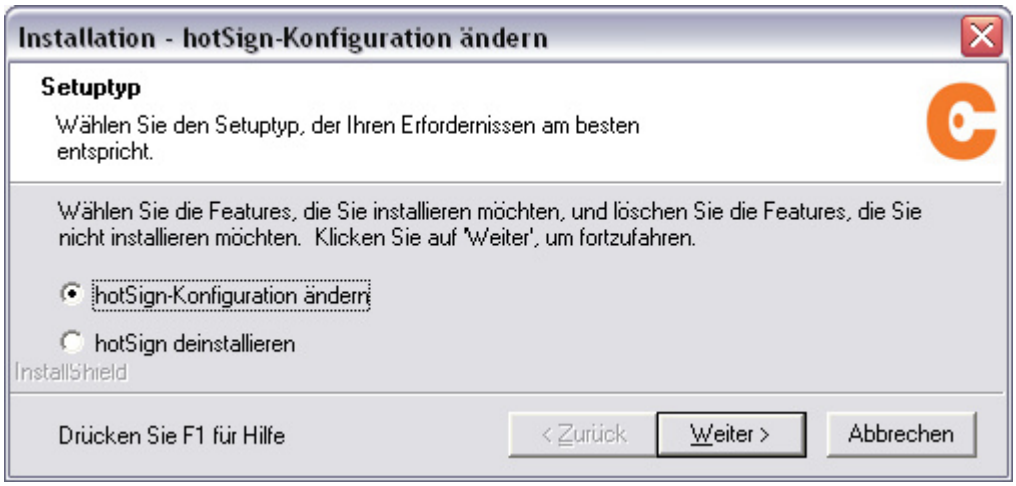


Figure 21: hotSign – hotSign-Konfiguration ändern

5. Weitere Vorgangsweise wie Kapitel 6.2 (Erstinstallation)

7.4. Grundsätzliches zur Kartenlesegeräten und Interfaces

Es gibt grundsätzlich zwei unterschiedliche Treibermodelle bzw. Interfaces für Kartenlesegeräte. Es handelt sich um

a) CT-API sowie um
b) PC/SC

Dabei ist es möglich, dass für ein und dasselbe Kartenlesegerät sowohl ein CT-API als auch ein PC/SC – Treiber verfügbar ist.

hotSign untertützt sowohl CT-API als auch PC/SC – Leser, wobei auf Grund der Vielzahl der möglichen Treiber nicht jeder Treiber mit **hotSign** getestet werden kann. Natürlich ist die Möglichkeit nicht auszuschließen, dass ein Benutzer ein Kartenlesegerät benutzen will, welches mit **hotSign** nicht getestet wurde und deshalb nicht freigegeben ist.

Die Verwendung eines solchen Kartenlesers ist zwar möglich, sofern es sich um einen **PC/SC**-Leser handelt, jedoch kann die fehlerfreie Funktion von **hotSign** nicht gewährleistet werden.

7.5. Deinstallation

1. Beenden von **hotSign**
2. Ausführen des **hotSign** Installationsprogrammes, oder Aufruf des Setups mit Hilfe der Softwareumgebung von Windows (**hotSign** in der Liste der bereits installierten Software auswählen)
3. „**hotSign** deinstallieren“ auswählen:

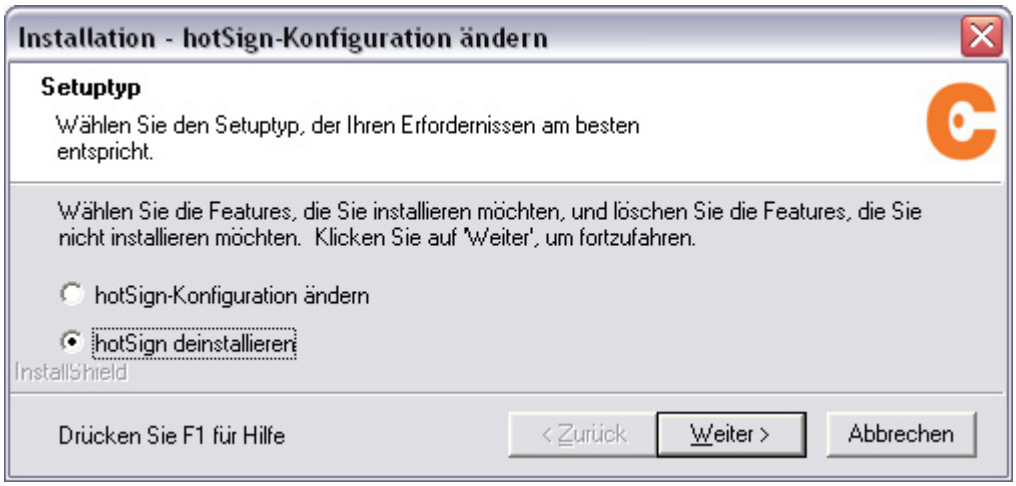


Figure 23: hotSign – Deinstallation

4. Deinstallation von hotPDFVerify für Adobe Reader
   Wurde das Plugin hotPDFVerify für Adobe Reader während der Installation von **hotSign** installiert, haben Sie nun die Möglichkeit dieses wieder von Ihrem System zu entfernen. Wenn Sie hotPDFVerify deinstallieren möchten, wählen Sie „Deinstallieren…“ und der Installationsassistenz von hotPDFVerify wird gestartet, der Sie durch den Deinstallationsvorgang führen wird. Wenn Sie das Adobe Plugin weiter verwenden möchten, wählen Sie „Überspringen“.

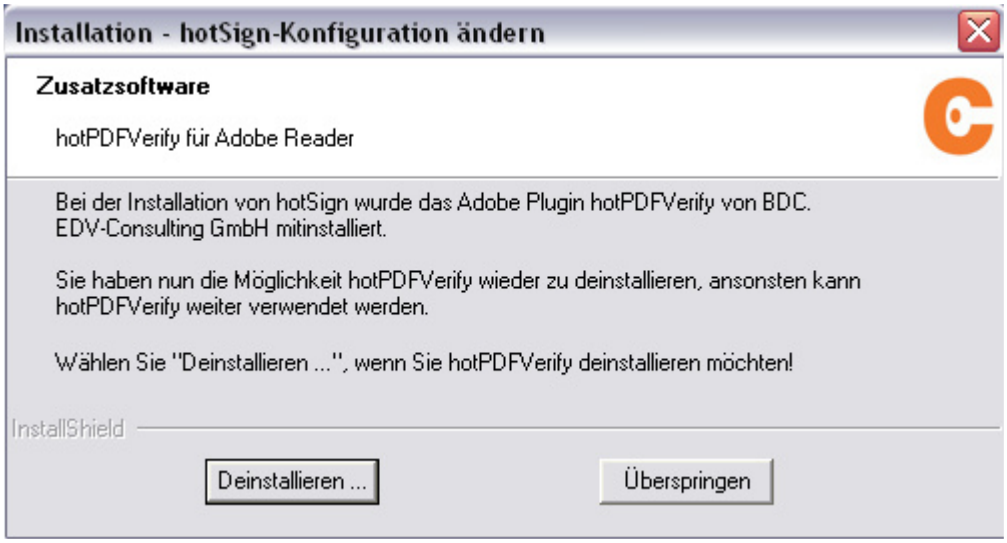


Figure 26: hotPDFVerify – Deinstallation

5. Die Deinstallation von **hotSign** ist beendet:

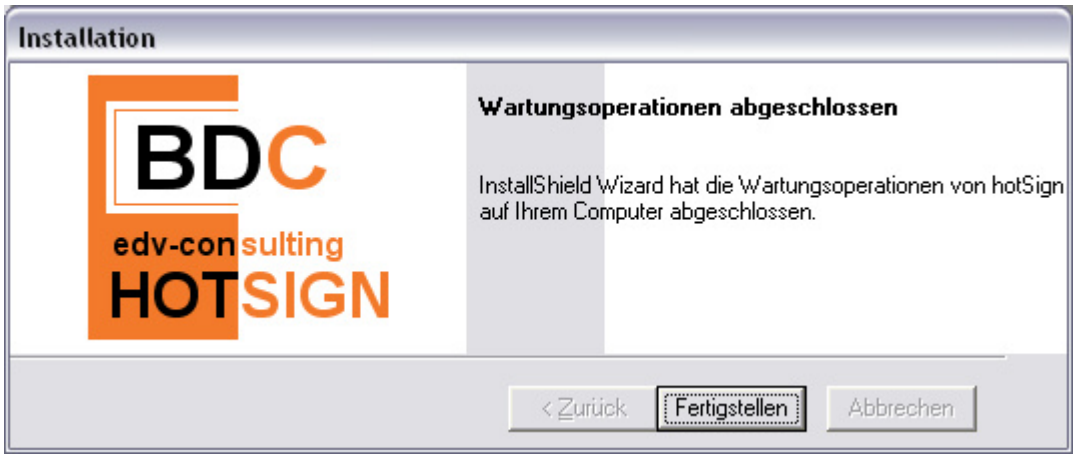


Figure 27: hotSign – Deinstallation beendet

8. Allgemeine Informationen zur Bürgerkartenumgebung

8.1. Grundlagen zur Signatur und Zertifikaten

Eine **digitale Signatur** ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, welches mit Hilfe eines zugehörigen öffentlichen Schlüssels den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt. Dabei muss der öffentliche Schlüssel mit einem Signaturschlüssel-Zertifikat eines **Zertifizierungsdienstanbieters** (Trustcenter) versehen sein.

Die **Signaturkarte** enthält ein oder mehrere digitale Schlüsselpaare, die aus einem privaten und einem öffentlichen Schlüssel besteht. Der private und der öffentliche Schlüssel samt Zertifikat bilden zusammen die elektronische Identität des Benutzers. Der private Schlüssel ist geheim und nur seinem Besitzer bekannt. Er kann auch nur von diesem genutzt werden. Der zertifizierte (von einem Trustcenter bestätigte) öffentliche Schlüssel eines Nutzers ist frei zugänglich und wird in allgemein zugänglichen Verzeichnissen allen Teilnehmern des Public-Key-Verfahrens zur Nutzung z.B. für Signaturprüfungen bereitgestellt.

Ein **Zertifikat** ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer bestimmten Person.

Ein **Zertifizierungsdienstanbieter** (Trustcenter) bescheinigt die Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen. Die digitalen Zertifikate werden von den Truscentern auf Signaturkarten gespeichert. Diese Signaturkarten sind mit einer PIN-Nummer geschützt, die nur dem Benutzer bekannt ist und die dieser jederzeit ändern kann. Um eine digitale Signatur zu erzeugen, benötigt man entsprechende Signaturkarten, Software (zB Bürgerkartenumgebung) und ein Kartenlesegerät.

Im Falle einer **bürgerkartenfähigen Signaturkarte** befinden sich zwei **Zertifikate** mit den entsprechenden **digitalen Schlüsselpaaren** auf der Signaturkarte:

- **Zertifikat für einfache Signatur** (Schlüsselpaar geschützt mit Geheimhaltungs-PIN bzw. Karten-PIN)
- **Zertifikat für qualifizierte Signatur** (Schlüsselpaar geschützt mit Signatur-PIN)

Für die Erstellung einer qualifizierten Signatur ist die **Signatur-PIN** erforderlich. Im Gegenzug, ist für die Erstellung einer einfachen Signatur die **Geheimhaltungs-PIN bzw. Karten-PIN** erforderlich.
Das Geheimhaltungsschlüsselpaar wird auch oft für die Verschlüsselung von Daten herangezogen.

8.2. Die Bürgerkarte

Weitreichende Informationen sind online über den link:

http://www.buergerkarte.at

abrufbar.

8.3. Infoboxen der Bürgerkarte

Die Bürgerkarten-Umgebung enthält Datenspeicher (Infoboxen), in die Applikationen Daten ablegen bzw. aus denen Applikationen Daten abrufen können. Im Rahmen des Konzeptes der Bürgerkarte werden folgende Infoboxen unterstützt:

8.3.1. Infobox für Zertifikate

Diese Infobox enthält Zertifikate, die mit den Signaturschlüsseln des Bürgers zusammenhängen. Mindestens standardmäßig verfügbar:

– Zertifikat für qualifizierte Signatur (Signaturschlüsselpaar)
– Zertifikat für einfache Signatur(Geheimhaltungsschlüsselpaar)

8.3.2. Infobox für die Personenbindung

Diese Infobox enthält die Personenbindung des Bürgers. Dies ist jener von der Stammzahlenregisterbehörde elektronisch signierte Datensatz, der die Stammzahl des Bürgers an die Zertifikate der Signaturschlüssel des Bürgers bindet. (Personenbindung standardmäßig verfügbar)

8.3.3. Infobox für Vollmachten

Diese Infobox enthält Vollmachten des Bürgers. Eine Vollmacht ist die Delegation von Rechten des Vollmachtgebers an den/die Vollmachtnehmer. Vereinfacht dargestellt enthält die Vollmacht durch den Vollmachtgeber signierte Informationen über ihn, den Vollmachtnehmer sowie den Vollmachtszweck.

8.4. Formate der signierten Daten

Der integrierte Secure-Viewer (zur Anzeige der zur Signatur vorgesehenen Daten) der Bürgerkartenumgebung **hotSign** ist in der Lage, die Formate:

- **XHTML** (inkl. Bilddaten)
- **Plain–Text**
- X**ML**

sicher darzustellen.

Sichere Darstellung bedeutet, dass sämtliche zur Signatur vorgesehenen Daten angezeigt werden, also keine sich unter Umständen dynamisch verändernden Inhalte mit-signiert werden..

8.5. Security-Layer

- Die Security Schnittstelle bzw. **Security-Layer** ist die Bezeichnung der Schnittstelle selbst. Sie stellt das Interface der Bürgerkarten-Umgebung zu Anwendungen dar und ist als XML-Schnittstelle ausgeführt.
- Die **Bürgerkarten-Umgebung** (**hotSign**) ist das eigentliche Programm (Service), welches unter anderem die Kommunikation mit der Bürgerkarte übernimmt, eine vertrauenswürdige Anzeige im Sinne des Signaturgesetzes, Signaturverifikationsfunktionen, etc. enthält.
- Die **Bürgerkarte** ist ein Token (z.B. Smartcard) der entpsrechend den Anforderungen des Konzeptes zur Bürgerkarte die notwendige Funktionalität bereitstellt.

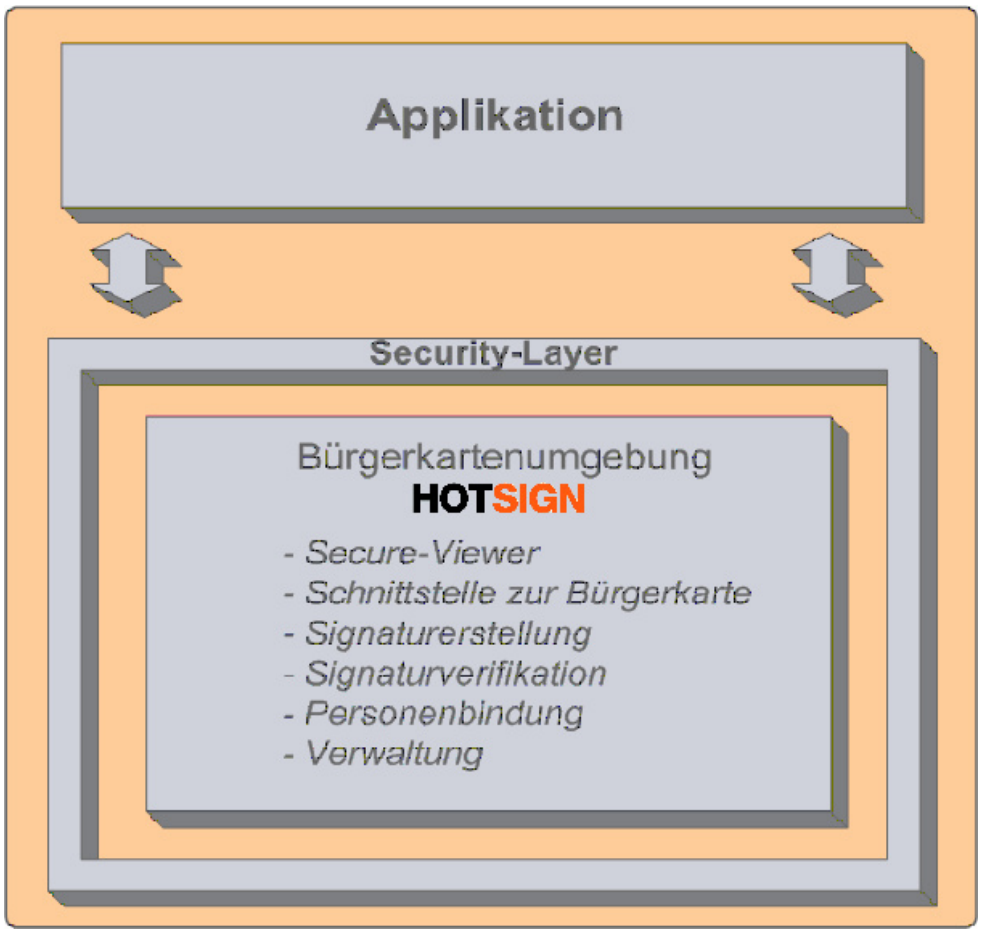


Figure 28: Security-Layer

8.6. Ablaufbeispiel

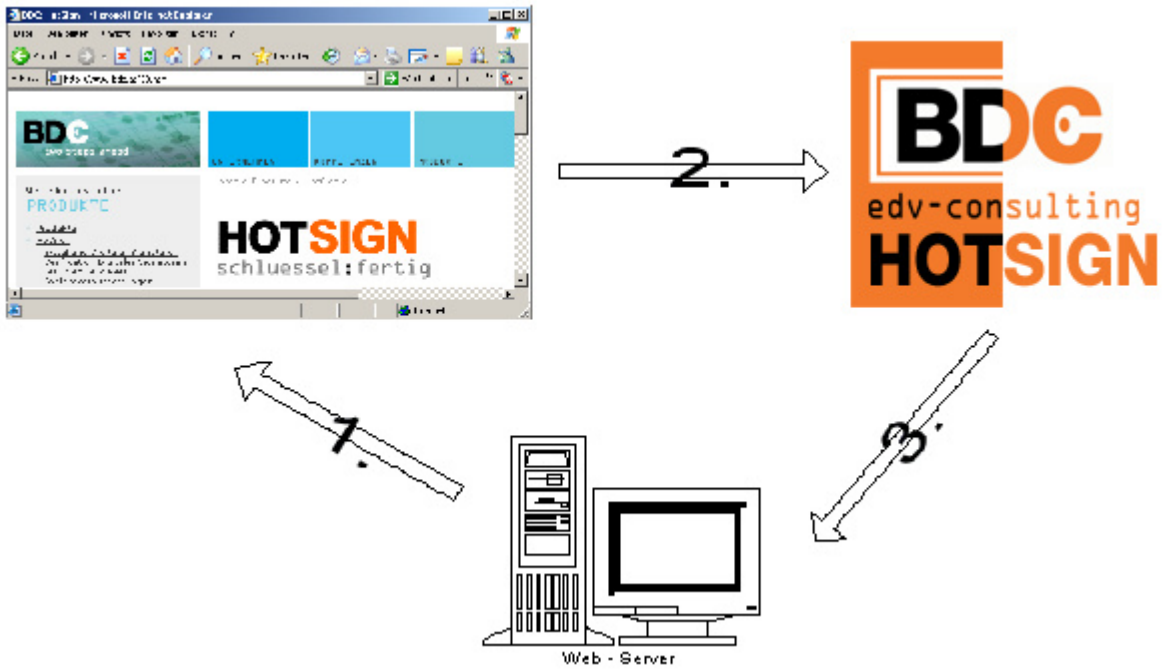


Figure 29: hotSign – Ablaufbeispiel

1. Ein Web–Server erstellt eine Webseite und sendet diese an den Web–Browser. Dort wird dem Benutzer zB ermöglicht Daten in ein Formular einzugeben.
2. Diese Informationen werden in ein SL-Kommando verpackt und an die Bürgerkartenumgebung (**hotSign**) gesendet. **hotSign** übernimmt anschließend die Verarbeitung (zB Signaturerstellung).
3. Die Antwort (zB Signatur) wird wieder an einen Web–Server gesendet, der entsprechend reagiert und die weitere Verarbeitung vornimmt (zB neue Benutzereingaben ermöglicht).

8.7. Bürgerkarte FAQ

Zusätzliche Hilfe in Form von FAQ´s bezüglich der Thematik Bürgerkarte und digitale Signaturen können unter folgendem Link abgerufen werden:

- http://www.signatur.rtr.at/de/security/faq.html

9. Programmbeschreibung

9.1. Programmstart/Beenden

hotSign wird beim Systemstart automatisch gestartet. Ein Icon in der Systray-Leiste zeigt an, dass **hotSign** aktiv ist. Sollte **hotSign** nicht aktiv sein, so kann **hotSign** mittels Doppelklick auf das Desktop–Icon oder im Startmenü unter
„Startmenü" – "Programme" – "BDC. EDV-Consulting GmbH" "Bürgerkartenumgebung hotSign" **gestartet** werden:

Figure 30: hotSign – Startmenü

Die Ausführung von **hotSign 2.0.0** kann vom Benutzer **beendet** werden, indem das **hotSign** –Menü mittels Rechtsklick auf das Systray–Icon geöffnet und danach auf „**hotSign** beenden" geklickt wird:

Figure 31: hotSign –Icon im Systray

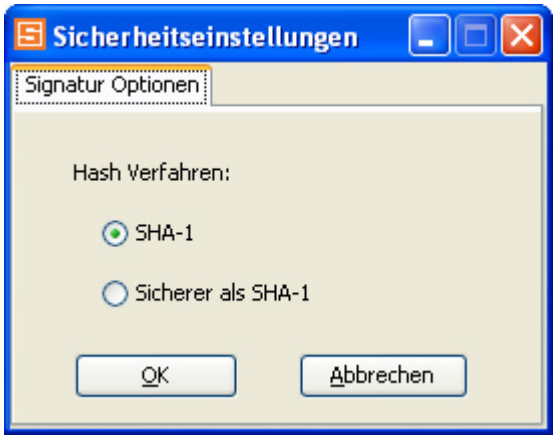
Splash-Screen

Bei jedem Aufruf von **hotSign** wird ein Splash-Screen angezeigt, der den Verarbeitungsstatus signalisiert. Da **hotSign** auch einen kaskadierenden Befehlsablauf unterstützt, wird der Splash-Screen möglicherweise mehrmals angezeigt und wieder geschlossen:

Figure 32: hotSign –Splash Screen

9.1. Hash Verfahren auswählen

Hash-Verfahren sind ein wichtiger Bestandteil bei der Signaturerstellung. Hierfür existieren einige unterschiedliche technische Verfahren (zB: SHA-1, SHA-256, Ripemd-160, etc.). In den vergangenen Jahren wurde zum Großteil SHA-1 benutzt. Dieses Verfahren ist allerdings in letzter Zeit ins Fadenkreuz der Kritik gelangt, da aufgezeigt wurde, dass die Sicherheit dieses Verfahrens u. U. in den nächsten Monaten / Jahren kompromittiert werden könnte. Zum aktuellen Zeitpunkt gibt es keine akute Bedrohung, dennoch sind Hersteller angehalten in ihren Produkten alternative (bessere) Verfahren zu unterstützen.
Die Interoperabilität zu anderen Systemen (zB: Bankrechner im E-Banking oder eGovernment-Applikationen) ist jedoch nur gewährleistet, wenn auch die zentralen Systeme diese Verfahren unterstützen. Dies ist zum aktuellen Zeitpunkt noch nicht in vollem Umfang gegeben. hotSign unterstützt deshalb auf expliziten Wunsch auch nach wie vor SHA-1. Der Benutzer kann dies im Dialogfenster „Sicherheitseinstellungen“ (Menü Verwaltung – Sicherheitseinstellungen) konfigurieren. Standardmäßig ist die Option „Sicherer als SHA-1“ ausgewählt. Sollte es mit einer Anwendung Probleme geben, da diese nur SHA-1 unterstützt, kann die Option „SHA-1“ ausgewählt werden. Wir weisen jedoch ausdrücklich darauf hin, dass dies aufgrund der Sicherheitsproblematik der Ausnahmefall sein sollte.



Wird „Sicherer als SHA-1“ ausgewählt, werden sicherheitsmäßig bessere Hash-Verfahren verwendet.

9.2. Erstellen einer Signatur

Die **hotSign**–Funktion „Erstellen einer Signatur“ erfüllt alle Auflagen des österreichischen Signaturgesetzes bezüglich des Erstellens qualifizierter Signaturen.

9.2.1. Durchführung

Um eine Signatur erstellen zu können, ist eine Applikation erforderlich, welche die zur Signatur vorgesehenen Daten an **hotSign** übermittelt.

Beispiel:

Eine Bank könnte die Möglichkeit zum Kauf/Verkauf von Aktien über das Internet anbieten und zu diesem Zweck ein Formular zur Aufnahme der Transaktionsdaten bereitstellen, die gewünschten Daten über den Kauf/Verkauf sind vom Benutzer einzutragen. Der verwendete Browser zeigt nach vollständiger Übermittlung der Daten an den Server der Bank nochmals eine Zusammenfassung der Transaktion an und bietet, zum Beispiel in Form eines Buttons, die Möglichkeit zur Weiterleitung der Daten zur Signatur.

Sobald der Benutzer die Daten zur Signatur weitergeleitet hat, wird **hotSign** aktiv. Es wird nun überprüft, ob tatsächlich eine Karte im Kartenleser steckt. Kann keine Karte gefunden werden, wird ein Dialog präsentiert, welcher den Benutzer bittet, eine Signatur–Karte in den Kartenleser zu stecken:

Figure 33: Aufforderung eine Karte in den Kartenleser zu stecken

hotSign zeigt die zur Signatur vorgesehenen Daten in einer sicheren Umgebung (Secure–Viewer) an. Dieser Secure–Viewer stellt sicher, dass ausschließlich die angezeigten Daten signiert werden. Falls sich die Daten nicht vollständig, also in einem Stück auf dem Bildschirm, darstellen lassen, so benutzt der Secure–Viewer Scrollbars ("Rollbalken"), mit deren Hilfe Sie die Daten im Secure–Viewer positionieren können.

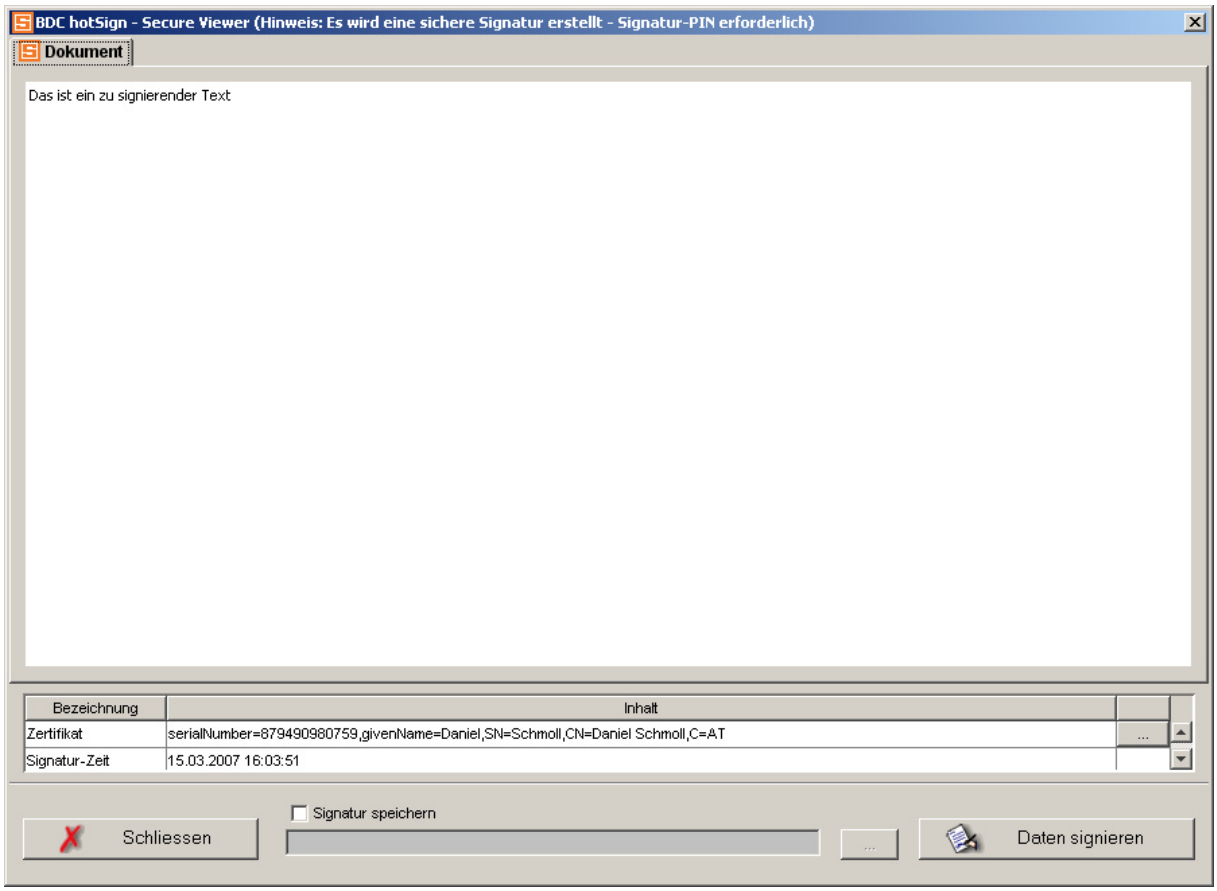


Figure 34: hotSign Secure-Viewer

Sollen **mehrere Dokumente in einem Signaturvorgang signiert** werden, wird eine entsprechende Anzahl von Register angezeigt (durch klicken auf die Register werden die entsprechenden Dokumente angezeigt) :

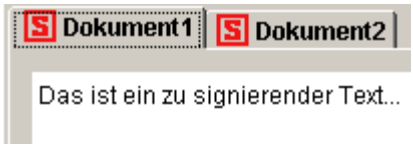


Figure 35: Zwei Dokumente zur Unterzeichnung

In der Menüleiste des Secure–Viewers wird angezeigt, ob eine qualifizierte bzw. eine einfache Signatur erstellt wird:

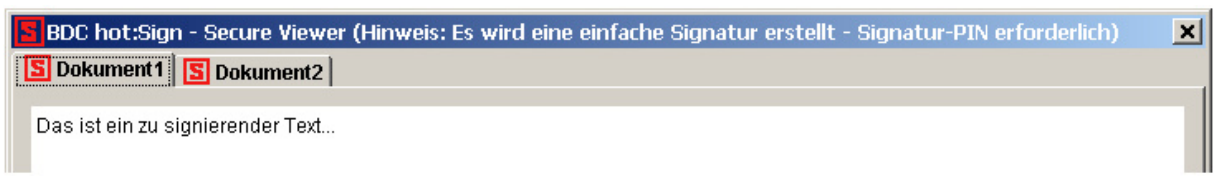


Figure 36: Es wird eine einfache Signatur erstellt

Des Weiteren wird in der Menüleiste angezeigt, **welcher PIN** (Signatur-PIN bzw. Geheimhaltungs-PIN) für die Signaturerstellung **erforderlich ist**.

Der Secure–Viewer in der Leiste unterhalb des Content-Fensters zeigt auch Informationen zum Signatur–Zertifikat sowie Zeitpunkt und Datum an, dabei handelt es sich um den Zeitpunkt zu dem der Secure Viewer geöffnet wurde (diese Information wird auch in die Signatur mit aufgenommen):

Bezeichnung	Inhalt	
Zertifikat	serialNumber=273137351600,givenName=Bernd,SN=Wittmann,CN=Bernd Wittmann,C=AT	...
Signatur-Zeit	20.11.2003 17:05:32	

Figure 37: Informationen zum Signatur–Zertifikat sowie Zeitpunkt und Datum

Detaillierte Informationen über das Zertifikat können mittels Klick auf den Button neben der Statuszeile "..." angefordert werden:

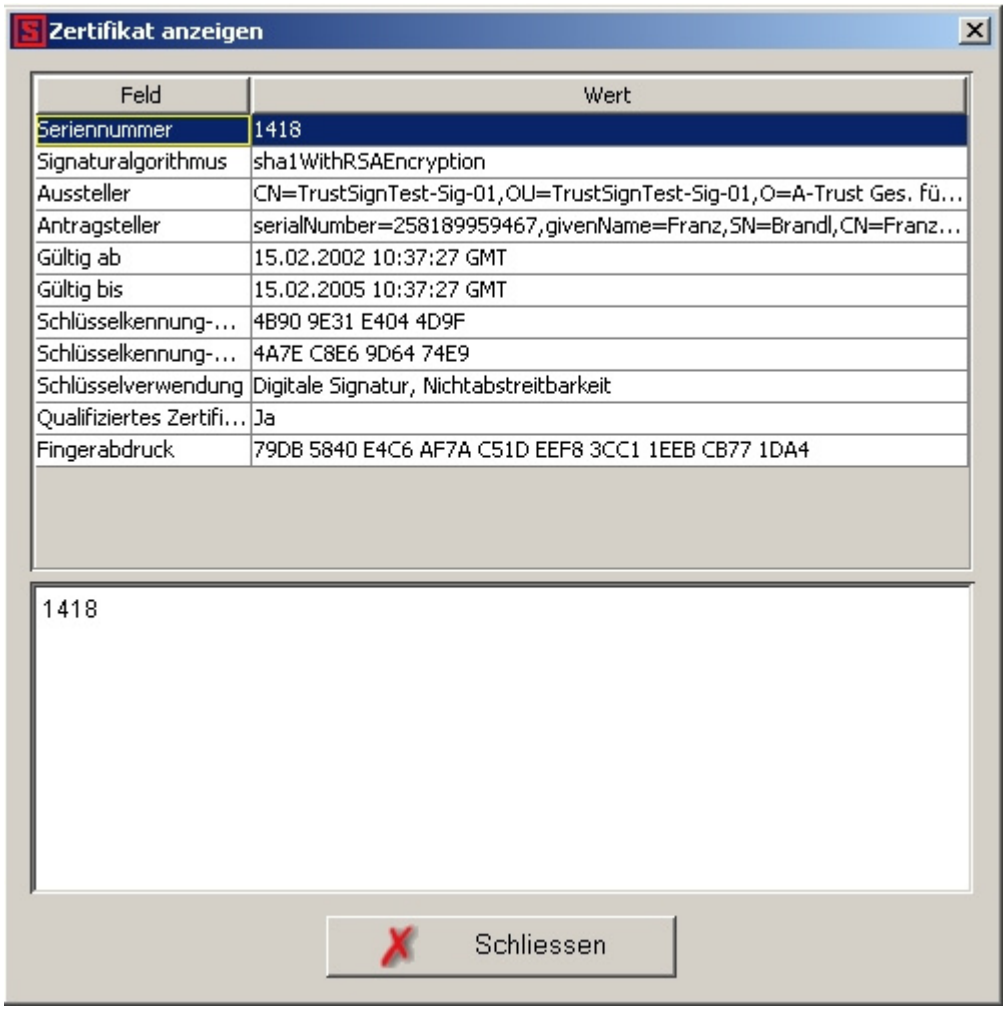


Figure 38: Erstellen einer Signatur - Informationen über das benutzte Zertifikat

Des Weiteren bietet **hotSign** eine Möglichkeit, die erzeugte Signatur zusätzlich lokal zu speichern. Dafür ist der Kontrollhaken "Signatur speichern" zu aktivieren und mit Hilfe des Buttons "..." (neben dem aktivierten Eingabefeld) kann jetzt ein Dateiname und Speicherort für die Signatur ausgewählt werden:

Figure 27: Signatur speichern

Nach Kontrolle der im Secure–Viewer angezeigten Daten und Überprüfung von Signaturdatum und Signaturzeit kann die Signatur mittels Klick auf den Button "Signieren" ausgelöst werden. Der Benutzer wird anschließend aufgefordert, die PIN am Kartenleser einzugeben. Nach Eingabe einer gültigen PIN werden die Daten signiert. Das Erstellen einer Signatur kann durch Drücken des "Schliessen"-Buttons jederzeit abgebrochen werden.

Die Signatur-Erstellung ist damit abgeschlossen. Eine Rückmeldung über den Status der Transaktion liegt in der Zuständigkeit der aufrufenden Applikation. Die Beschreibung der Benutzerführung ist der Dokumentation der Signatur–Anwendung zu entnehmen.

9.2.2. Mögliche Fehlerursachen

Während dem Signatur-Vorgang mit **hotSign** können folgende Fehler auftreten:

- Falsche Eingabe der Signatur–PIN
- Signatur–PIN blockiert
- Keine Karte im Kartenlesegerät
- Timeout bei der PIN-Eingabe
- Kein Kartenleser
- Keine geeignete Signatur-Karte
- Unerwarteter Fehler

Eventuell auftretende Fehlermeldungen werden der aufrufenden Applikation übermittelt – eine weitere Fehlerbehandlung liegt in der Zuständigkeit derselben.

9.3. Signaturverifikation

Bei einer Signaturverifikation wird zuerst der Signaturwert überprüft (Integritätsprüfung). Anschließend erfolgt eine Überprüfung des Zertifikats, das bei der Signaturerstellung verwendet worden ist. Dabei wird unter anderem eine LDAP–Verzeichnisdienstabfrage durchgeführt um die Zertifikatskette (Zusammenhang zwischen vertrauenswürdigen Root-Zertifikat und dem vorliegenden Zertifikat) aufzulösen und zu überprüfen. Zusätzlich werden Widerrufsinformationen in die Signaturverifikation einbezogen.

9.3.1. Durchführung

Sofern die Signatur mit **hotSign** erfolgreich verifiziert wurde und es sich um anzeigbare Daten handelt (siehe Kapitel 8.4 Formate der signierten Daten), werden die signierten Daten dargestellt und das Ergebnis der Zertifikatsüberprüfung angezeigt (Wenn die Daten nicht anzeigbar sind, erfolgt keine Darstellung).

Bei einer erfolgreichen Zertifikatsüberprüfung wird folgendes Fenster angezeigt:

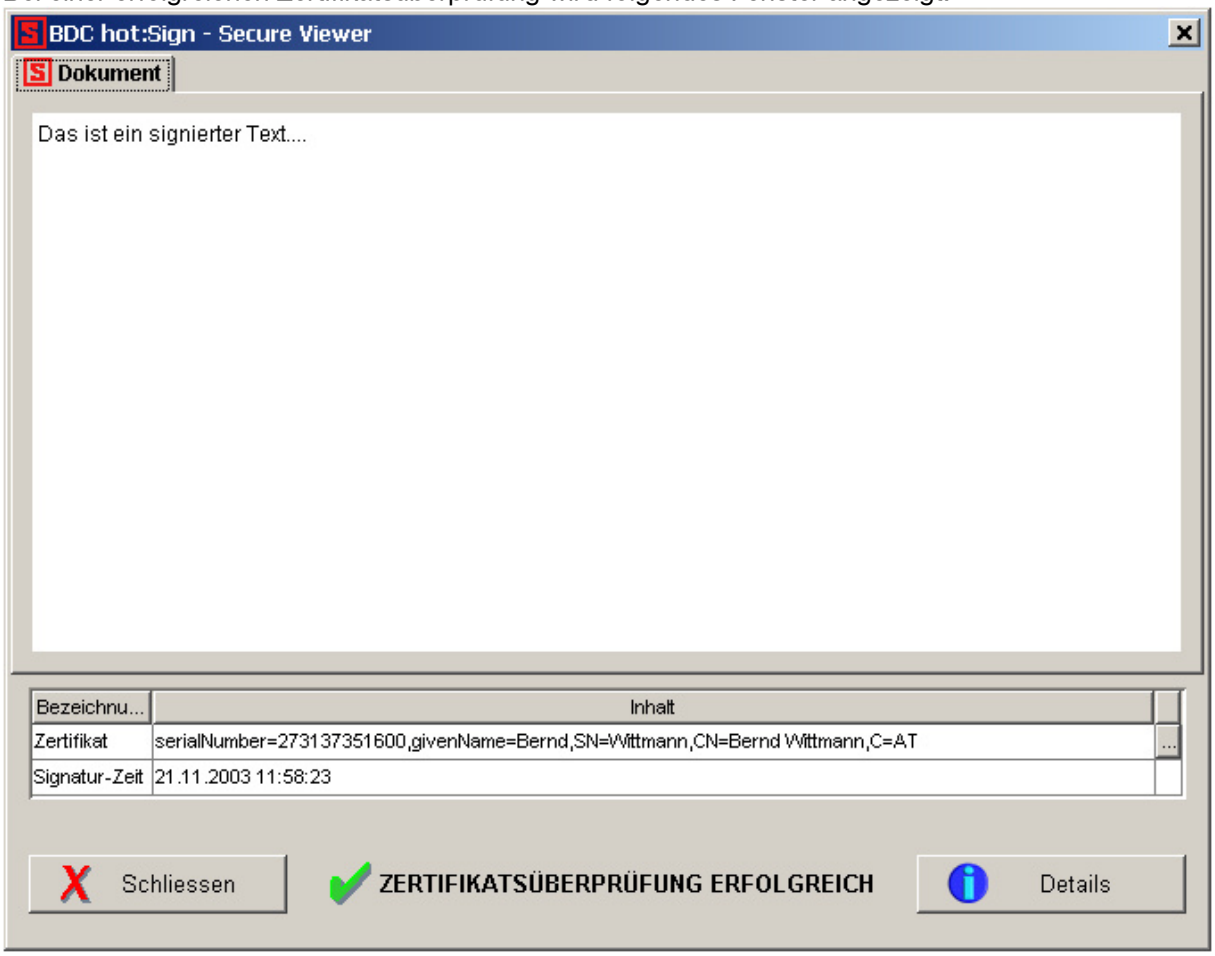


Figure 39: Erfolgreiche Zertifikatsüberprüfung

Durch betätigen des Button "Details" wird (bei einer erfolgreichen Zertifikatsüberprüfung) folgende Meldung angezeigt:

Figure 40: Ergebnis der Zertifikatskettenüberprüfung

Detaillierte Informationen über das Zertifikat (mit dem die Signatur erstellt worden ist) können mittels Klick auf den Button neben der Statuszeile "..." angefordert werden:

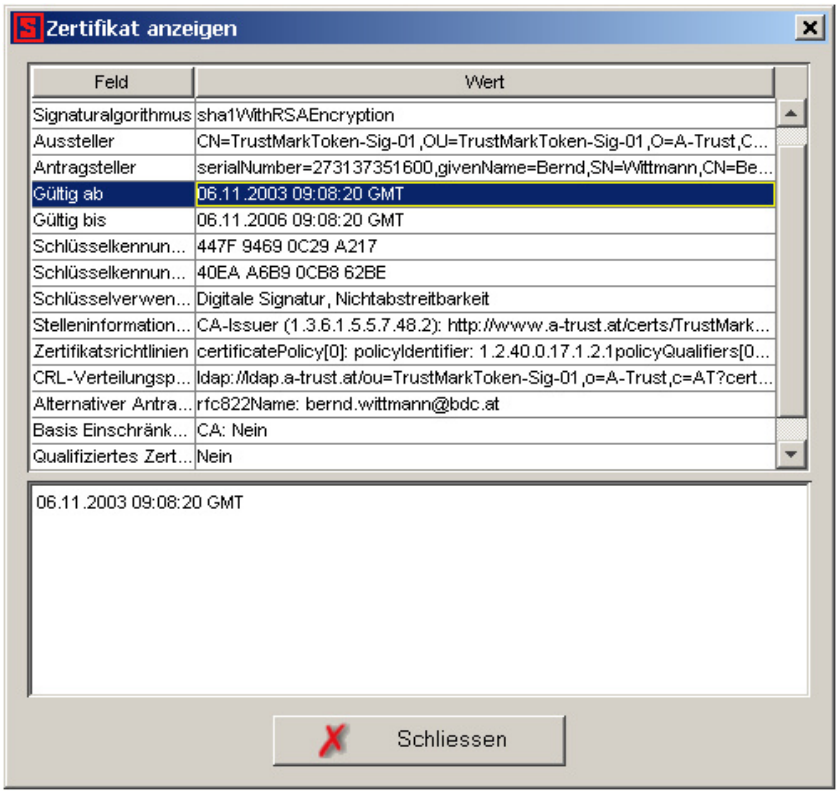


Figure 41: Verifizieren einer Signatur - Informationen über das benutzte Zertifikat

Konnte die Zertifikatsüberprüfung **nicht** erfolgreich durchgeführt werden wird folgendes Fenster angezeigt:

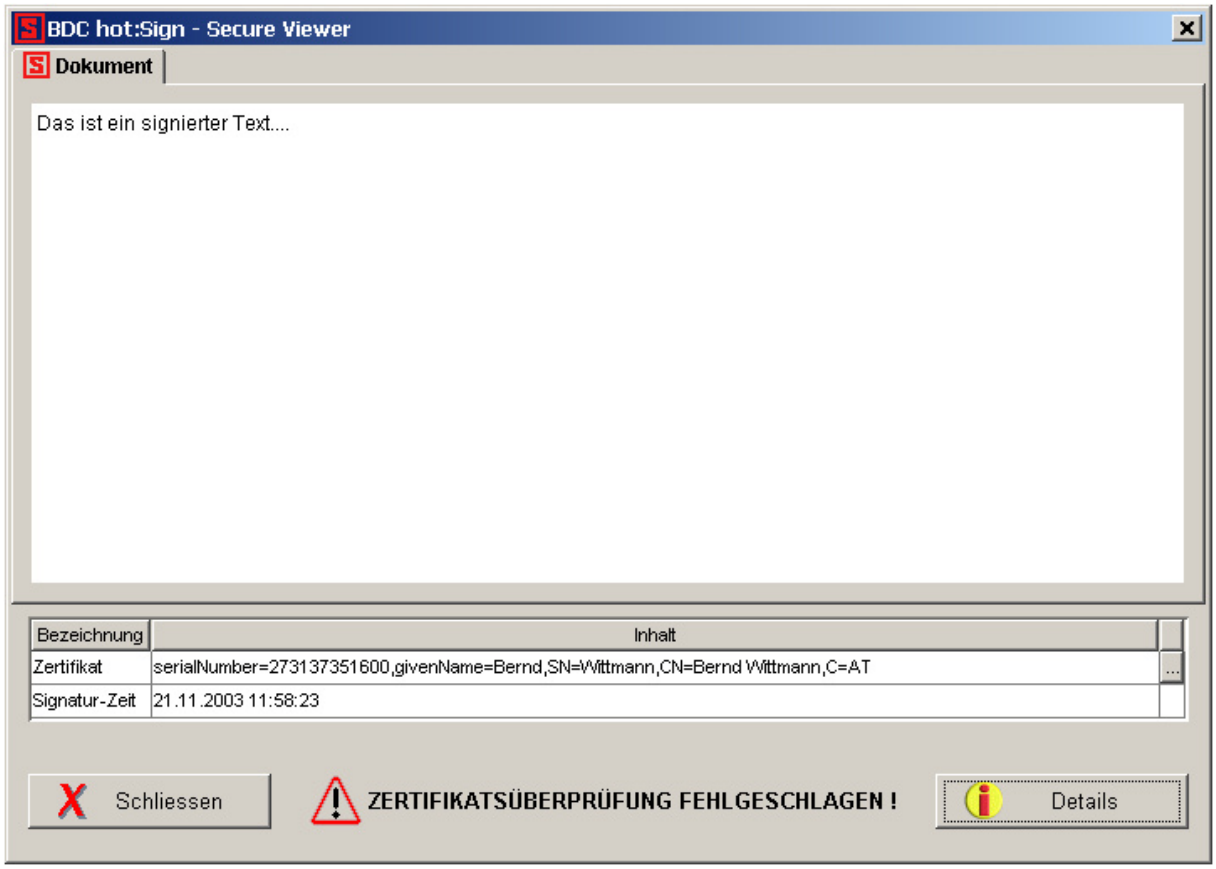


Figure 42: Zertifikatsüberprüfung fehlgeschlagen

Mehr Informationen zur Zertifikatsüberprüfung kann mit Hilfe des Button "Details" erlangt werden, zB:

Figure 43: Ergebnis der Zertifikatskettenüberprüfung

9.3.2. Mögliche Fehlerursachen

Folgende Fehlermeldungen sind möglich:

- Die Zertifikatskette konnte erfolgreich aufgelöst werden, jedoch ist mindestens ein Zertifikat dieser Kette zum Prüfzeitpunkt ungültig!
- Die Zertifikatskette konnte erfolgreich aufgelöst werden, alle Zertifikate dieser Kette sind zum Prüfzeitpunkt gültig, jedoch konnte für zumindest ein Zertifikat dieser Kette der Zertifikatstatus nicht festgestellt werden!
- Die Zertifikatskette konnte erfolgreich aufgelöst werden, alle Zertifikate dieser Kette sind zum Prüfzeitpunkt gültig, jedoch ist zumindest ein Zertifikat dieser Kette zum Prüfzeitpunkt widerrufen!
- Die Zertifikatskette konnte erfolgreich aufgelöst werden, alle Zertifikate dieser Kette sind zum Prüfzeitpunkt gültig, kein Zertifikat dieser Kette ist zum Prüfzeitpunkt widerrufen, jedoch ist zumindest ein Zertifikat zum Prüfzeitpunkt gesperrt!

9.4. hotSign Module

9.4.1. PIN ändern

Das **hotSign** Modul „PIN ändern“ erfüllt alle Auflagen des österreichischen Signaturgesetzes bezüglich des „sicheren“ Änderns einer Signatur–PIN. Mittels Rechtsklick auf das Systray–Icon wird das **hotSign** -Menü geöffnet, danach auf „**hotSign** Module - PIN ändern" klicken um das Modul zu öffnen. Daraufhin erscheint ein entsprechender Hinweisdialog welcher PIN geändert werden kann, bzw. ein Auswahlmenü welche PIN geändert werden soll:

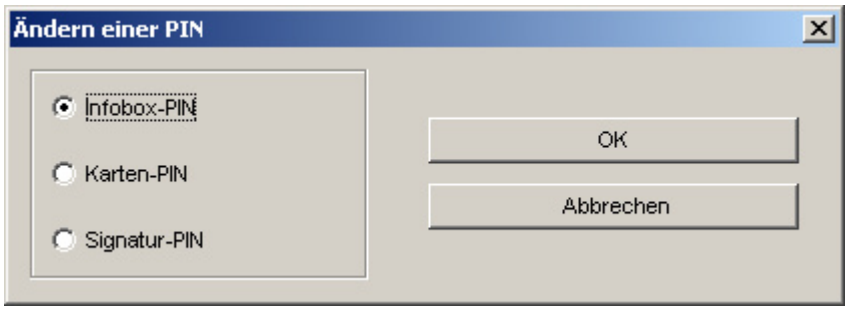


Figure 44: Auswahl – PIN ändern

hotSign sucht nun nach einem angeschlossenen unterstützten Kartenleser. Nachdem dieser gefunden wurde, überprüft **hotSign**, ob sich eine geeignete Signatur–Karte im Kartenleser befindet. Ist dies nicht der Fall, wird der Benutzer aufgefordert, eine Signatur–Karte in den Kartenleser zu stecken:

Figure 45: Aufforderung eine Karte in den Kartenleser zu stecken

Kann keine Karte gefunden werden, wird der Dialog neuerlich präsentiert. Nachdem eine Signatur–Karte gefunden wurde, wird der folgende Dialog angezeigt der den Benutzer darauf hinweist, dass jetzt die Signatur–PIN am PIN–Pad des Kartenlesers geändert werden kann:

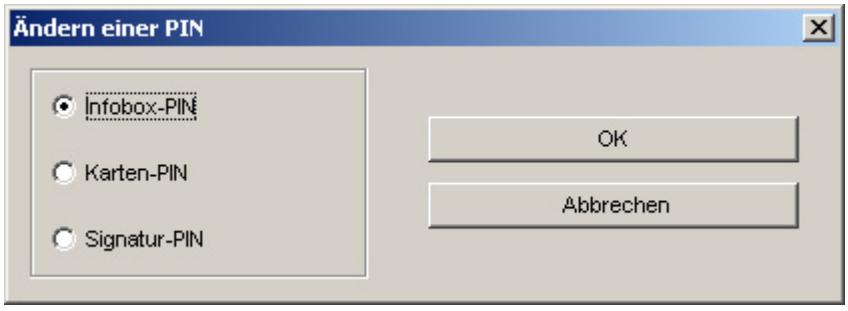


Figure 46: Ändern der Signatur - PIN

Der Titel der Dialogbox und der Inhalt weisen auf das benutzte Kartenlesegerät hin. Das Ändern der Signatur–PIN kann durch Drücken des „Abbrechen“-Buttons jederzeit abgebrochen werden.
Das Ändern der PIN erfordert vom Benutzer, dass dieser zuerst die alte Signatur–PIN am Kartenleser eingibt, danach ist die gewünschte neue Signatur–PIN zweimal einzugeben. Die gewünschte neue Signatur–PIN muss mindestens sechs Zeichen lang sein. Wenn die beiden neuen PIN´s identisch sind, wird der Inhalt der Signatur–PIN geändert. Konnte die Signatur–PIN geändert werden, wird die Meldung „Die PIN wurde erfolgreich geändert“ am Bildschirm angezeigt.

Figure 47: PIN erfolgreich geändert

Mögliche Fehlerursachen

Das **hotSign** Tool „Ändern der Signatur–PIN“ wertet verschiedene Fehlerzustände von **hotSign** aus. Während dem Ändern der Signatur-PIN können folgende Fehler auftreten:

Falsche Eingabe der Signatur–PIN

Wird während dem Ändern der Signatur-PIN die ursprüngliche PIN falsch eingegeben, wird die Anzahl der weiteren möglichen Versuche dem Benutzer gemeldet:

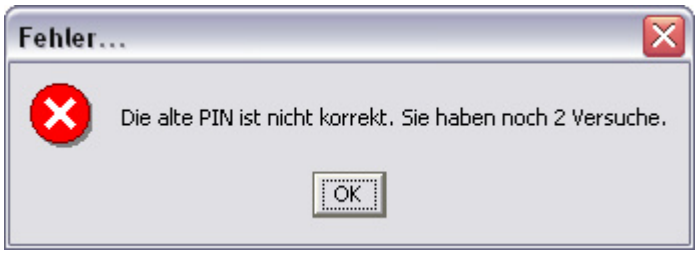


Figure 48: Ändern der Signatur–PIN–Eingabefehler

Falsche Eingabe der gewünschten neuen PIN

Ist die gewünschte neue PIN bei der wiederholten Eingabe nicht identisch, wird diese Tatsache dem Benutzer mitgeteilt:

Figure 49: Ändern der Signatur-PIN–Eingabefehler

Die Anzahl der weiteren möglichen Versuche die Signatur–PIN zu ändern, wird durch diese falsche Eingabe nicht verändert.

Signatur–PIN blockiert

Ist die Signatur-PIN (durch eine wiederholt falsche Eingabe) gesperrt, wird eine Änderung der Signatur-PIN nicht mehr ermöglicht:

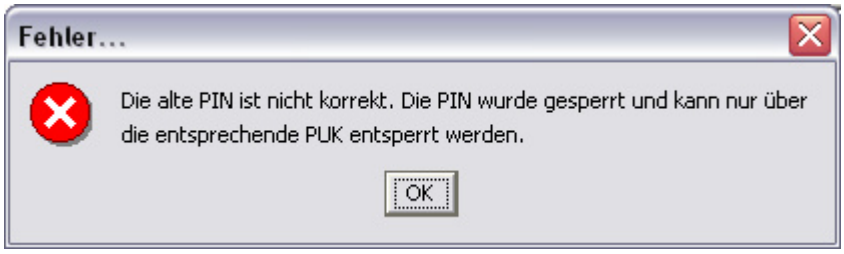


Figure 50: Ändern der Signatur–PIN – PIN gesperrt

Timeout

Die PIN's müssen innerhalb einer gewissen Zeitspanne eingegeben werden. Verstreicht diese Zeitspanne, bricht das Terminal das Ändern der Signatur-PIN ab:

Figure 51: Ändern der Signatur– PIN – Timeout

Kein Chipkarten-Terminal gefunden

Wurde kein geeignetes Chipkarten-Terminal gefunden (nicht angeschlossen, bzw. der entsprechende Treiber ist fehlerhaft oder nicht installiert), kann das Ändern der Signatur-PIN nicht durchgeführt werden:

Figure 52: Ändern der Signatur-PIN - Kein Terminal vorhanden

Keine geeignete Signatur-Karte

Ist die eingelegte Karte keine geeignete Signaturkarte, oder tritt während der Kommunikation mit der Karte ein Problem auf, wird die Funktion abgebrochen:

Figure 53: Ändern der Signatur-PIN – Keine geeignete Karte

Unerwarteter Fehler

Diese Meldung erscheint, wenn ein aufgetretener Fehler in keine der obigen Kategorien fällt:

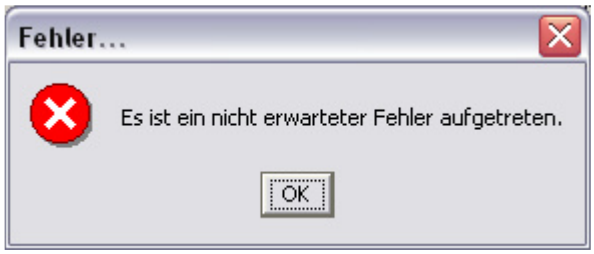
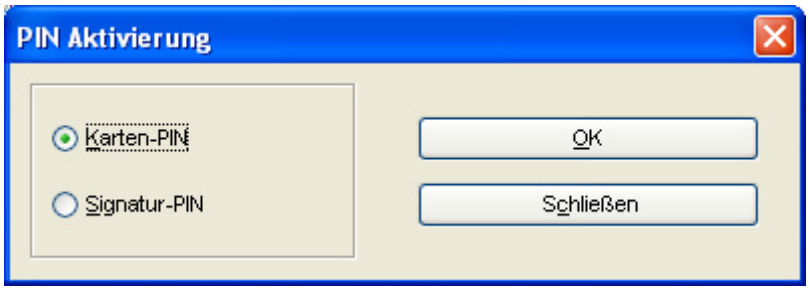


Figure 54: Ändern der Signatur-PIN - Nicht erwarteter Fehler

9.4.2. PIN aktivieren

Diese Funktion ist nur für die Benutzung der eCard als Signaturkarte relevant. Im Zuge der Freischaltung der eCard als Signaturkarte müssen die PINs der Karte „aktiviert“ werden. Darunter versteht man die erstmalige Festlegung der PINs.
Wenn Sie im Zuge der Freischaltung der Signatur dazu aufgefordert werden, benutzen Sie bitte diese **hotSign** Funktion.

Klicken Sie zunächst mit der rechten Maustaste auf das Systray–Icon von **hotSign** und danach auf „**hotSign** Module - PIN aktivieren":



Die „Karten-PIN“ ist bereits ausgewählt. Klicken Sie auf die Schaltfläche OK, um die Karten-PIN festzulegen.

Achtung: Bestimmte Kartenlesegeräte erlauben die PIN-Aktivierung am Pinpad des Kartenlesers. Es handelt sich dabei um folgende Geräte:

- Reiner SCT cyberJack pinpad
- Reiner SCT cyberJack e-Com
- SCM SPR 532

- Cherry Smartboard

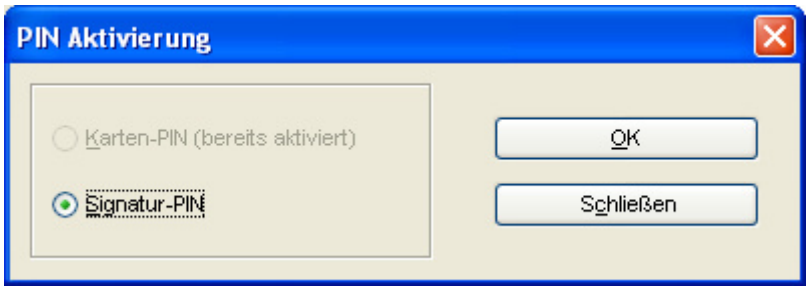
Alle anderen Kartenlesegeräte, insbesondere alle Kartenleser die über die PC/SC-Schnittstelle angesprochen werden, unterstützen die PIN-Aktivierung am Pinpad nicht. Die PINs müssen in diesem Fall auf der Tastatur eingegeben werden. Bitte beachten Sie unbedingt die Sicherheitshinweise Abschnitt 6 Hinweise.

Unterstützt Ihr Kartenlesegerät die PIN-Aktivierung auf dem Pinpad, befolgen Sie bitte die Anweisungen des Kartenlesers. Um Tippfehler zu vermeiden werden sie 2 Mal hintereinander zur Eingabe der PIN aufgefordert. Nur wenn diese identisch eingegeben werden, wird die PIN erfolgreich aktiviert.

Unterstützt Ihr Kartenlesegerät die PIN-Aktivierung auf dem Pinpad nicht, wird folgendes Dialogfenster angezeigt:

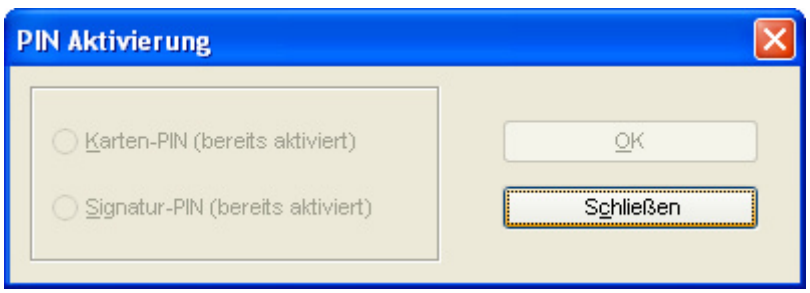
Geben Sie bitte 2 Mal die gewünschte PIN ein und klicken Sie anschließend auf OK. In der Folge wird eine Hinweismeldung angezeigt, dass die PIN erfolgreich aktiviert wurde. Bestätigen Sie diese mit OK.

Schließlich wird wieder folgendes Dialogfenster angezeigt:



Wiederholen Sie nun den Vorgang für die Signatur-PIN.

Wurde die Aktivierung dieser PIN ebenfalls erfolgreich abgeschlossen, wird folgender Dialog angezeigt:



Damit wurden alle PINs erfolgreich aktiviert. Bitte klicken Sie auf Schließen, um die PIN-Aktivierung zu beenden.

9.4.3. PIN entsperren

Mittels Rechtsklick auf das Systray–Icon wird das **hotSign** -Menü geöffnet, danach auf „**hotSign** Module - PIN entsperren" klicken um das Modul zu öffnen.
hotSign sucht nun nach einem installierten Kartenleser. Nachdem dieser gefunden wurde, überprüft **hotSign**, ob sich eine geeignete Signatur–Karte im Kartenleser befindet. Ist dies nicht der Fall, wird der Benutzer aufgefordert, eine Signatur–Karte in den Kartenleser zu stecken:

Figure 55: Aufforderung eine Karte in den Kartenleser zu stecken

Das Entsperren einer PIN kann durch Drücken des „Abbrechen"-Buttons abgebrochen werden. Kann keine Karte gefunden werden, wird der Dialog neuerlich präsentiert. Danach wird, **abhängig davon welche Signaturkarte** sich im Kartenleser befindet, ein entsprechender Dialog präsentiert:

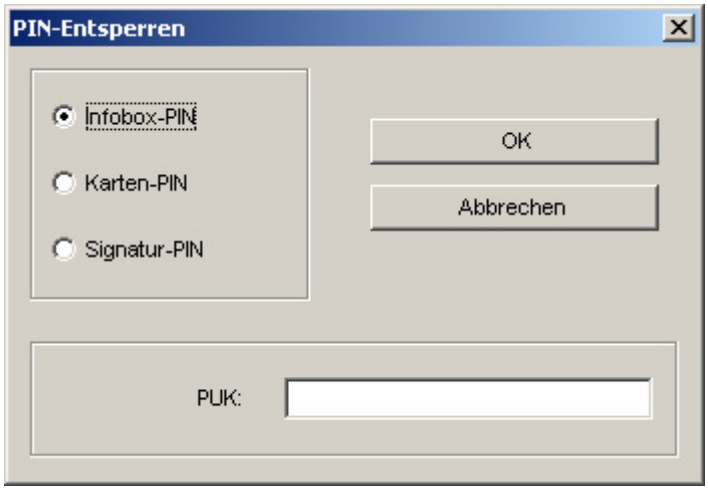


Figure 56: Entsperren einer PIN

Die zu entsperrende PIN wird mit Hilfe der Radiobuttons ausgewählt. Alle Zeichen der einzugebenen PUK werden als Stern (*) dargestellt.

Alle Zeichen der einzugebenden PINs und der einzugebenden PUK werden als Stern (*) dargestellt. Die einzugebende PIN wird zweimal abgefragt, erst wenn die beiden Eingabewerte der gewünschten neuen PIN identisch sind, wird das Entsperren der PIN durchgeführt.

Sicherheitshinweis: *Manche der benutzten Betriebsysteme können Fernwartungsfunktionen zur Verfügung stellen, mit deren Hilfe ein Angreifer die eingegebenen PUKs und PINs abhören kann.*

Wenn dem Benutzer nach dem Entsperren einer PIN die Karte gestohlen wird, kann ein Angreifer versuchen mit Hilfe der PUK die PIN zu erraten.

Mögliche Fehlerursachen

Das **hotSign** Tool „Entsperren einer PIN“ wertet mögliche Fehlerzustände von **hotSign** aus. Während dem Entsperren der PIN können folgende Fehler auftreten:

Falsche Eingabe der PUK

Wird während des Entsperren-Vorganges die PUK falsch eingegeben, wertet ein karteninterner Fehlerzähler die Anzahl der weiteren möglichen Versuche aus. **hotSign** meldet dem Benutzer die Anzahl der möglichen weiteren Versuche:

Figure 57: Entsperren einer PIN – Eingabefehler

PUK blockiert

Ist die PUK (durch eine wiederholt falsche Eingabe) blockiert, kann die entsprechende PIN nicht mehr entsperrt werden:

Figure 58: Entsperren einer PIN - PUK blockiert

Kein Chipkarten-Terminal gefunden

Wurde kein geeignetes Chipkarten-Terminal gefunden (nicht angeschlossen, bzw. der entsprechende Treiber ist fehlerhaft oder nicht installiert), kann das Entsperren der PIN nicht durchgeführt werden:

Figure 59: Entsperren einer PIN - Kein Terminal vorhanden

Keine geeignete Signatur-Karte

Ist die eingelegte Karte keine geeignete Signatur-Karte, oder tritt während der Kommunikation mit der Karte ein Problem auf, wird die Funktion abgebrochen:

Figure 60: Entsperren einer PIN - Keine geeignete Karte

Unerwarteter Fehler

Diese Meldung erscheint, wenn ein aufgetretener Fehler in keine der obigen Kategorien fällt:

Figure 61: Entsperren einer PIN - Nicht erwarteter Fehler

9.4.4. Beliebige Datei signieren/verifizieren

Mit den Modulen “Datei signieren” und „Datei verifizieren“ ist es möglich, eine beliebige Datei zu signieren und später diese Datei zu verifizieren.

Signieren

Mittels Rechtsklick auf das Systray–Icon und einem Bestätigen von „**hotSign** Module - Datei signieren" wird das entsprechende Fenster angezeigt:

Figure 62: hotSign – Datei Signieren

Mit Hilfe des Buttons “Durchsuchen” kann jetzt die zu signierende Datei ausgewählt werden. Weiters können Sie festlegen ob Sie eine einfache oder qualifizierte Signatur erstellen möchten. Sie steuern dies über die Checkbox „Qualifizierte digitale Signatur (Secure-Viewer)“.

Möglichkeit 1. Erstellung einer einfachen Signatur

Jede beliebige Datei bis zu einer Größe von 30MB kann signiert werden. Die erstellte Signatur wird mit Hilfe des Geheimhaltungsschlüsselpaars auf der Karte erstellt. Für die Erstellung ist die Eingabe der GeheimhaltungsPIN erforderlich.

Möglichkeit 2. Erstellung einer qualifizierten Signatur (Standardeinstellung)

Wenn die Checkbox " Qualifizierte digitale Signatur (Secure-Viewer)" aktiviert wird, versucht **hotSign** eine qualifizierte Signatur mit Anzeige des Secure-Viewers zu erstellen.
Folgende Dateiformate werden unterstützt:

- Text-Dateien im Format Latin-1 (ISO-8859-1)
- PDF – Dateien (falls das PDF-Modul aktiviert ist)

Nach Bestätigung des Buttons “Signieren” werden Sie aufgefordert den **Geheimhaltungs-PIN** (oder im Falle der Erstellung einer qualifizierten Signatur die **Signatur-PIN**) am Pin-Pad des Kartenlesegeräts einzugeben.

Text-Dateien

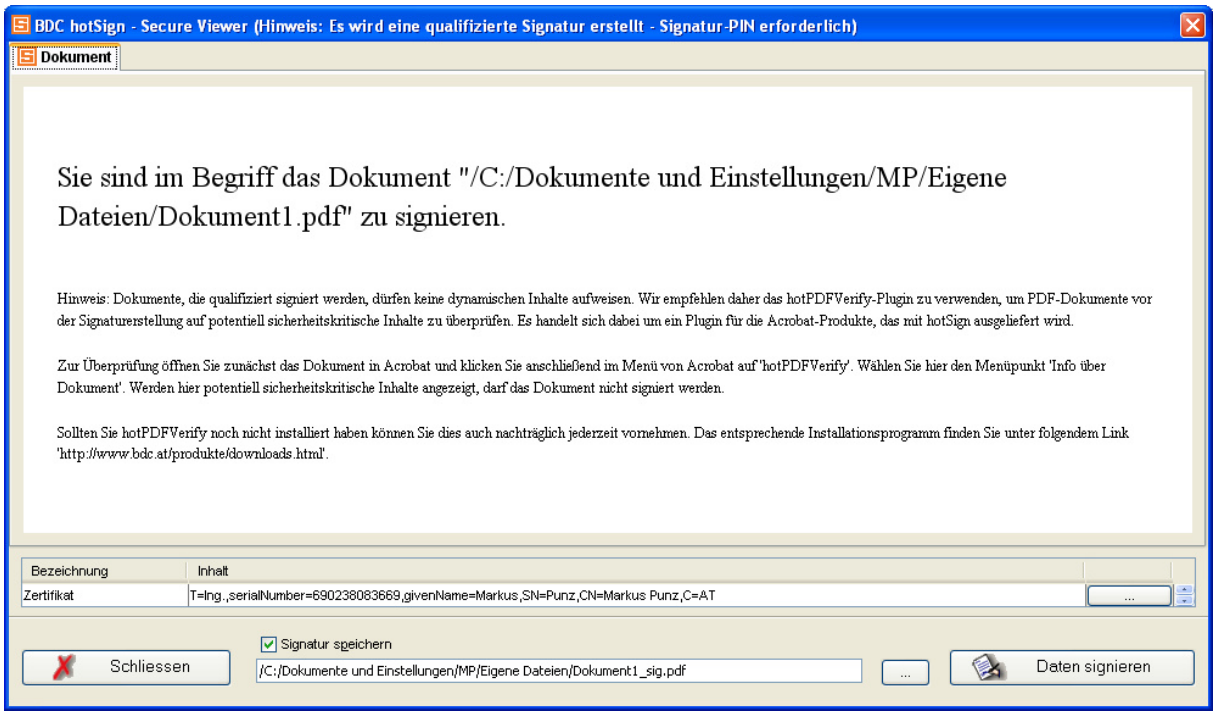
Bitte beachten Sie, dass in diesem Fall nur Text-Dateien im Format Latin-1 (ISO-8859-1) unterstützt werden. Der **Dateiinhalt** wird in jedem Fall **als „plain-text“ im Format Latin-1 interpretiert** und dargestellt. Für die Erstellung ist die Eingabe der SignaturPIN erforderlich (siehe Dialogtitel).

Hinweis: *Die Größe der zu signierenden Datei darf bei Erstellung einer* qualifizierten *Signatur 2MB nicht überschreiten (Secure-Viewer Beschränkung).*

PDF-Dateien

Bei Auswahl eines PDF-Dokuments wird überprüft ob sich „leere“ Signaturfelder im Dokument befinden (also Signaturfelder die noch keine Signatur enthalten). Die Namen der gefundenen Signaturfelder werden in der Liste „Signaturfeld auswählen“ angezeigt. Die Liste enthält immer das Element „Neues Signaturfeld“ – dieses ist standardmäßig ausgewählt.
Falls Sie ein bestehendes Signaturfeld auswählen wird die PDF-Signatur in der Folge in dieses Feld eingetragen. Falls im PDF-Einstellungsdialog ein Signatur-Icon aktiviert ist (siehe 10.4 PDF Konfiguration) wird auch das Signatur-Icon in das ausgewählte Feld eingetragen.
Wählen Sie „Neues Signaturfeld“ wird unabhängig von eventuell bereits bestehenden Signaturfeldern eine neues PDF-Signaturfeld erstellt. Die Position und Größe des Signaturfelds wird im PDF-Einstellungsdialog (siehe 10.4 PDF Konfiguration) festgelegt. Ist zudem ein Signatur-Icon aktiviert wird auch dieses eingetragen.

Der integrierte Secure-Viewer von hotSign unterstützt die Anzeige von PDF-Dateien nicht. Aus diesem Grund wird im Viewer-Fenster folgender Hinweis angezeigt:

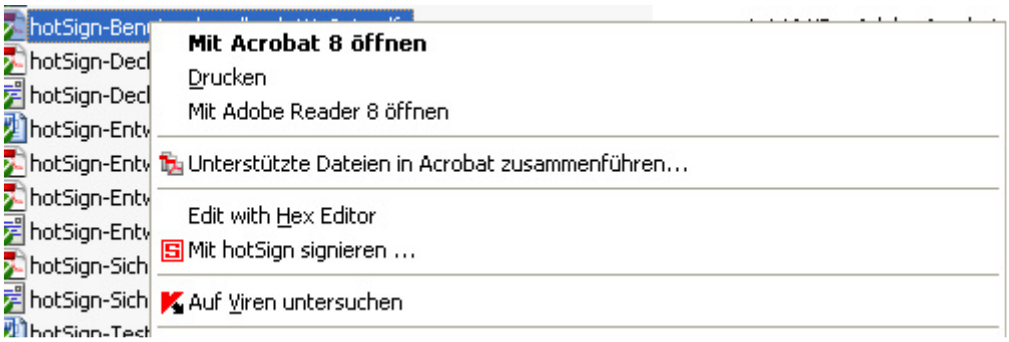


Achtung: Wir empfehlen ausdrücklich als Standard-Anwendung für die Anzeige von PDF-Dateien Acrobat Reader zu verwenden. In diesem Fall steht Ihnen das hotPDFVerify-Plugin zur Verfügung, um das zu signierende PDF-Dokument auf potentiell sicherheitskritische Inhalte zu überprüfen. Enthält das PDF-Dokument derartige Inhalte darf die Signaturerstellung nicht durchgeführt werden.

Die Checkbox „Signatur speichern“ ist standardmäßig aktiviert. Der Dateiname des PDF-Dokuments ist im darunterliegenden Eingabefeld mit dem Zusatz „_sig“ eingetragen. Wird das Dokument in der Folge signiert (Schaltfläche „Daten signieren“) wird das signierte PDF-Dokument unter diesem Dateinamen gespeichert. Dadurch wird verhindert, dass das ursprüngliche Dokument überschrieben wird. Eine Änderung des Dateinamens kann durch den Benutzer vorgenommen werden.

Context-Menü

Die Signatur von PDF-Dateien steht ebenfalls über das Context-Menü von Windows zur Verfügung. Klicken Sie dazu eine PDF-Datei (beispielsweise in Windows-Explorer) mittels Rechtsklick an. Im Context-Menü befindet sich der Eintrag „Mit hotSign signieren…“



In der Folge wird die Funktion „Datei signieren“ automatisch gestartet:

Der Name der ausgewählten PDF-Datei ist bereits eingetragen.

Verifizieren

Mittels Rechtsklick auf das Systray–Icon und einem Bestätigen von „**hotSign** Module“ - Datei verifizieren" wird das entsprechende Fenster angezeigt:

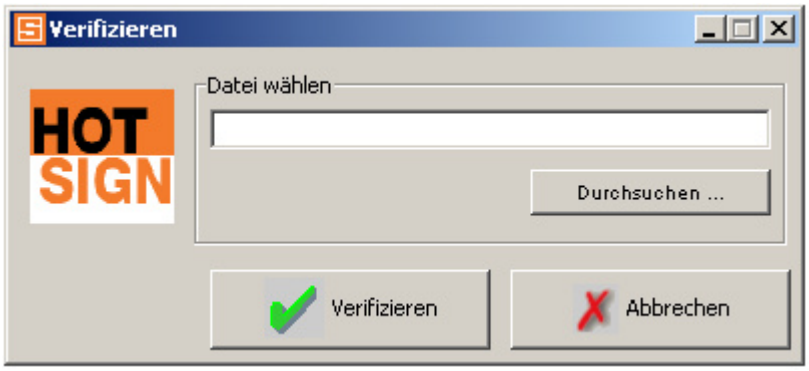


Figure 63: hotSign –Signaturdatei verifizieren

Mit Hilfe des Buttons “Durchsuchen” kann jetzt die Signaturdatei ausgewählt werden:

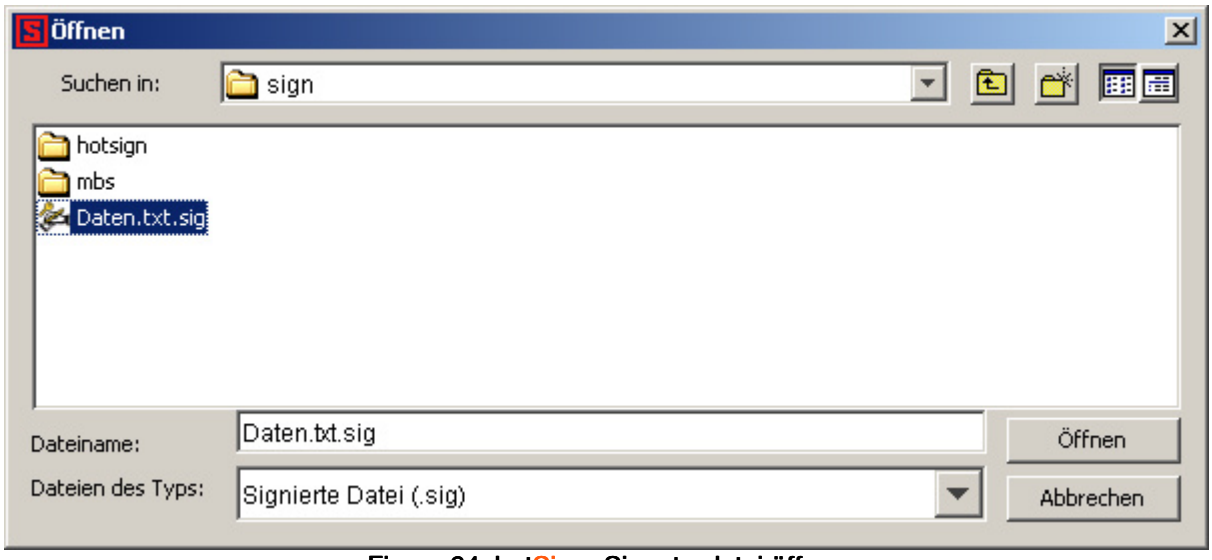


Figure 64: hotSign -Signaturdatei öffnen

Nachdem die Signaturdatei ausgewählt wurde beginnt der Verifizierungsvorgang von **hotSign**. Das Ergebnis der Signaturprüfung wird in einem entsprechenden Dialog angezeigt. Konnte zB der Zertifikatsstatus nicht ermittelt werden (wegen einer fehlenden Internetverbindung) wird folgender Dialog präsentiert:

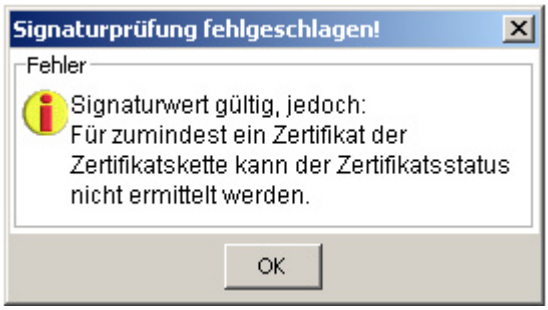


Figure 65: Signaturprüfung fehlgeschlagen

Ist das Ergebnis der **Signaturprüfung positiv** wird dieser Dialog angezeigt:

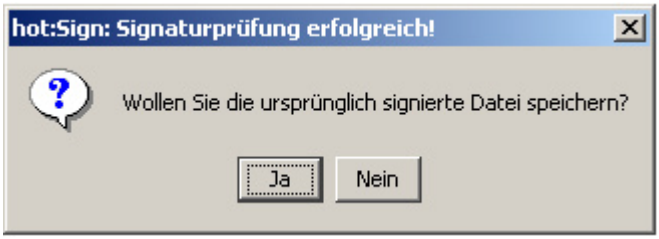


Figure 66: Signaturprüfung erfolgreich

Sie haben jetzt die Möglichkeit die ursprünglich signierte Datei zu speichern. Wenn Sie die Abfrage mit “Ja” beantworten wird ein Dialog angezeigt, wobei Sie den Speicherort und Dateinamen frei wählen können:

Figure 67: Signierte Daten anzeigen

9.4.5. Infoboxen anzeigen

Mit dem Programm-Modul “Infoboxen auslesen” ist es möglich die Personenbindung und die Zertifikate der Bürgerkarte auszulesen. Mittels Rechtsklick auf das Systray–Icon und einem Bestätigen von „hotSign Module“ Infoboxen anzeigen" wird das entsprechende Fenster angezeigt:

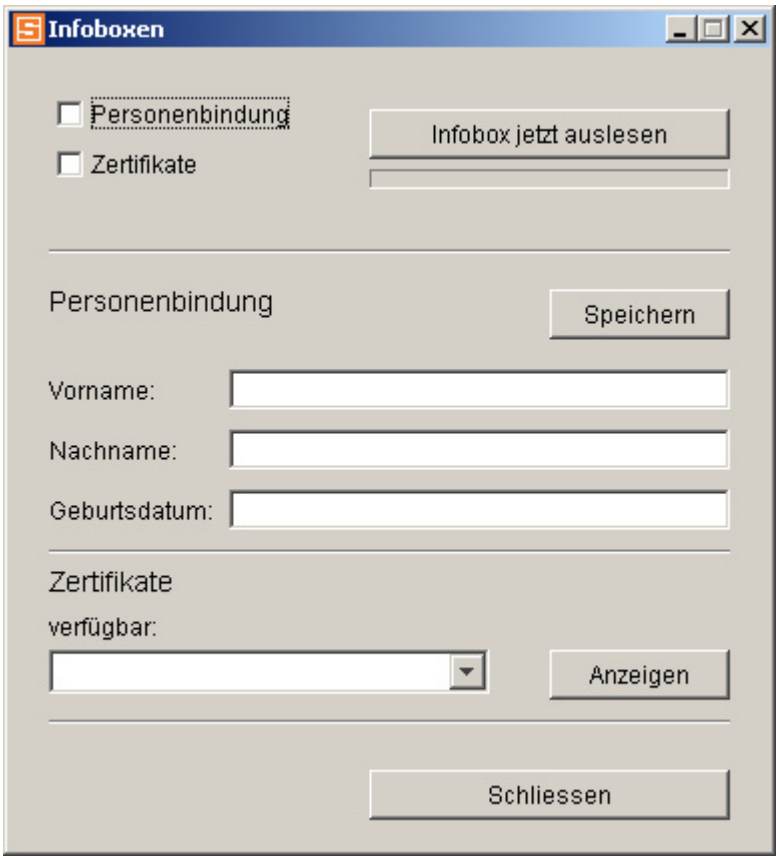


Figure 68: hotSign Infoboxen anzeigen

Es können gesondert die Personenbindung bzw. die auf der Bürgerkarte gespeicherten öffentlichen Zertifikate mit Hilfe des angeschlossenen Kartenlesegeräts ausgelesen werden. Dies erfolgt durch aktivieren der Checkbox für Personenbindung und/oder Zertifikate und anschließendem Betätigen des Buttons „Infobox jetzt auslesen“. Bei einer vollwertigen Bürgerkarte werden zB folgende Informationen angezeigt:

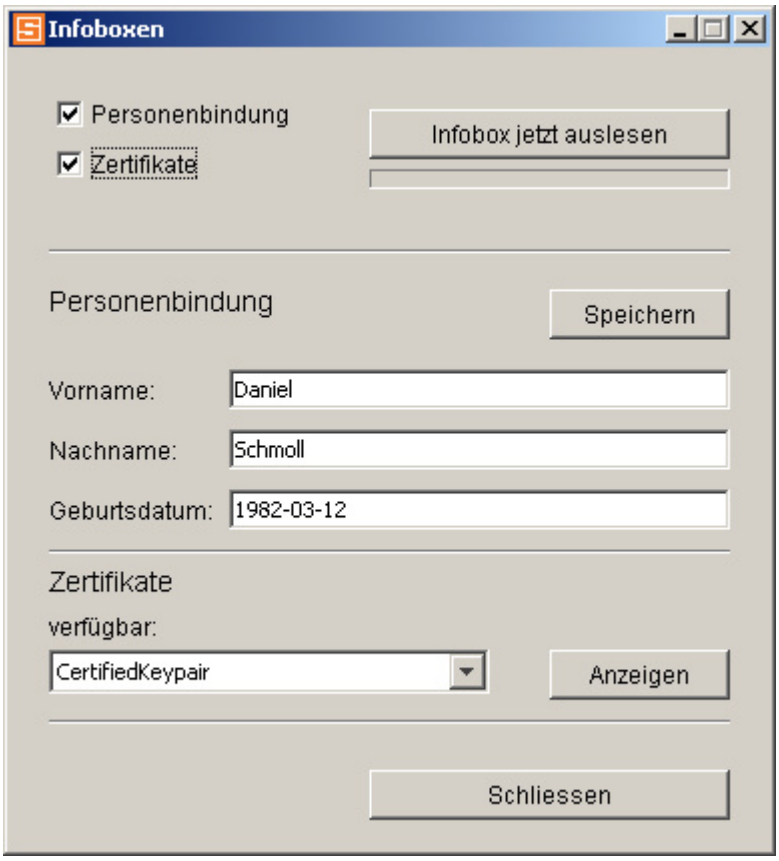


Figure 69: Infoboxen ausgelsen

Mit Hilfe des Buttons „Speichern“ kann die vollständige Personenbindung (xml-Format) gesondert gespeichert werden. Detaillierte Informationen zum ausgewählten Zertifikat erlangt man durch Betätigen des Buttons “Anzeigen”:

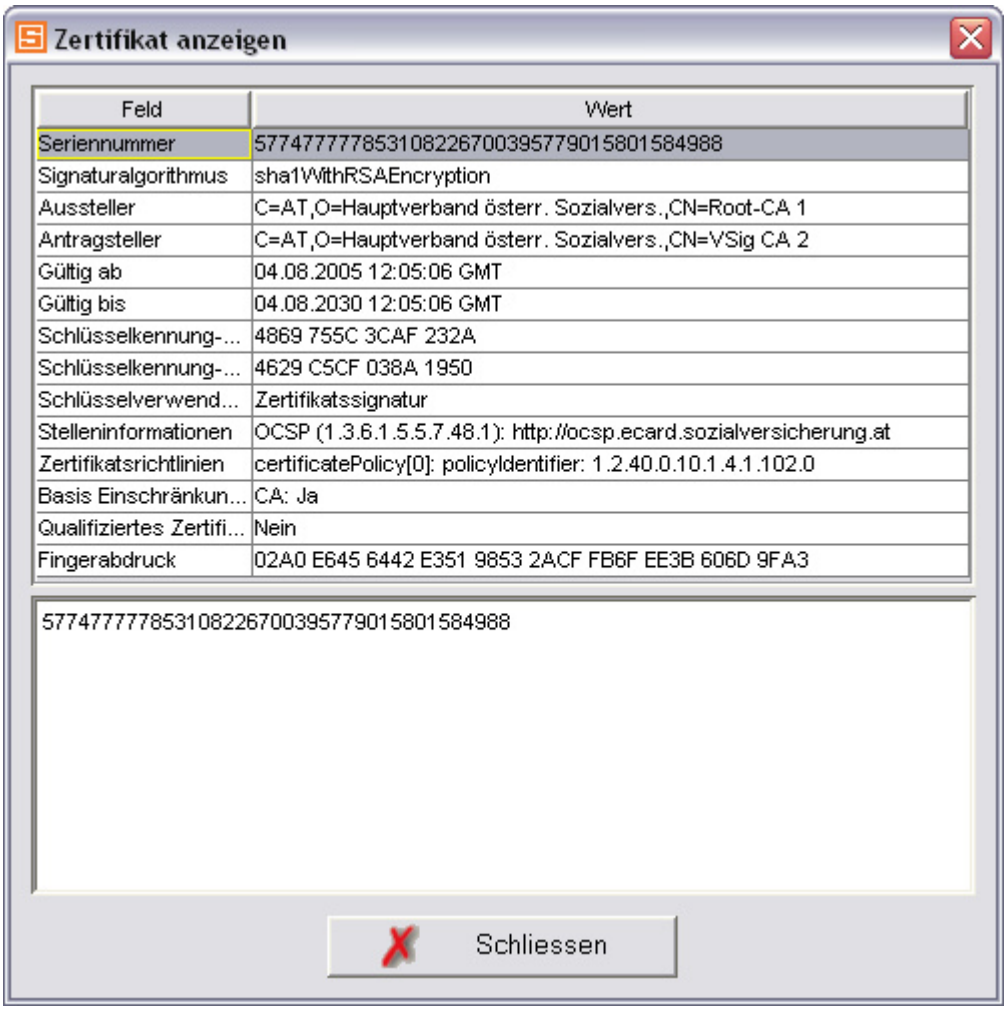


Figure 70: Zertifikat anzeigen

10. Verwaltungsfunktionen

10.1. Zertifizierungsinstanzen

Als Zertifizierungsinstanzen (kurz ZI oder auch Certificate Authority - kurz CA) genannt, werden Institutionen (in Österreich zB A-Trust) bezeichnet, welche Zertifikate ausgeben. Um qualifizierte Signaturen erstellen zu können, ist ein qualifiziertes Zertifikat erforderlich. Um die Gültigkeit eines Zertifikats überprüfen zu können, muss **hotSign** zur Ausführungszeit Informationen vom LDAP–Verzeichnisdienst abrufen. Hierfür benötigt **hotSign** einige LDAP–spezifische Zugangsdaten, welche mit einem entsprechenden Programm-Modul administriert werden können (Die Zugangsdaten werden von der Zertifizierungsinstanz ausgegeben).

Das **hotSign** –Menü mittels Rechtsklick auf das Systray–Icon öffnen, danach auf „Verwaltung“ – „Zertifizierungsinstanzen" klicken.

hotSign bietet verschiedene Funktionen zur Verwaltung von Zertifizierungsinstanzen an. In der Übersicht werden alle Verzeichnisdienste in Listenform angezeigt - die Anzeige beinhaltet Information über:

- Bezeichnung der Zertifizierungsinstanz

- URL des LDAP–Dienstes
- Benutzername sowie Passwort des Anwenders beim LDAP–Dienst.

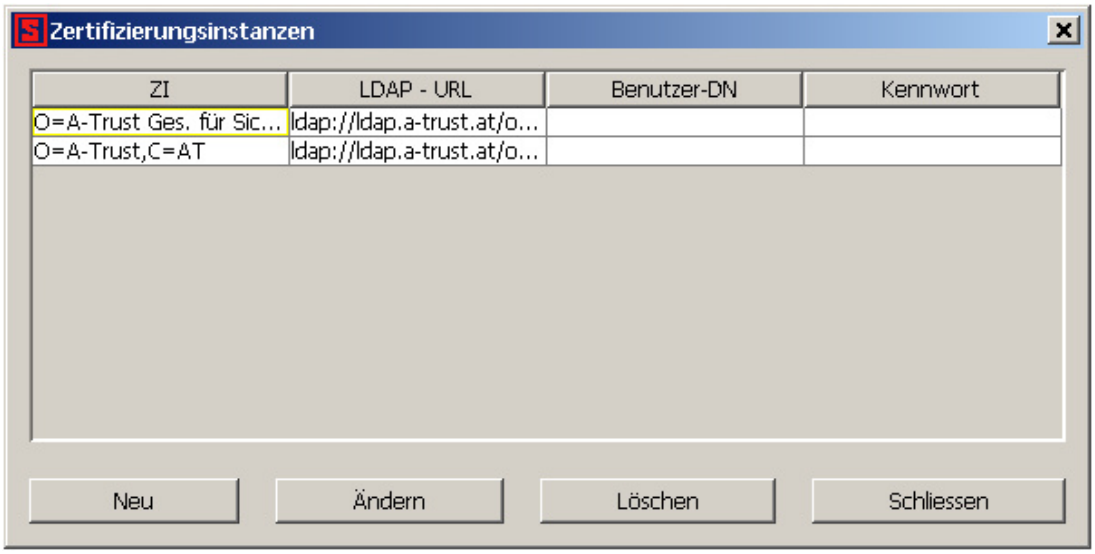


Figure 71: Zertifizierungsinstanzen - Übersicht

10.1.1. Zertifizierungsinstanz hinzufügen

Um eine neue Zertifizierungsinstanz hinzuzufügen, klickt man auf den Button "Neu". Es erscheint eine Eingabemaske zur Eingabe der LDAP–Zugangsdaten. Die Neueintragung kann durch klicken auf die entsprechenden Buttons gespeichert oder abgebrochen werden:

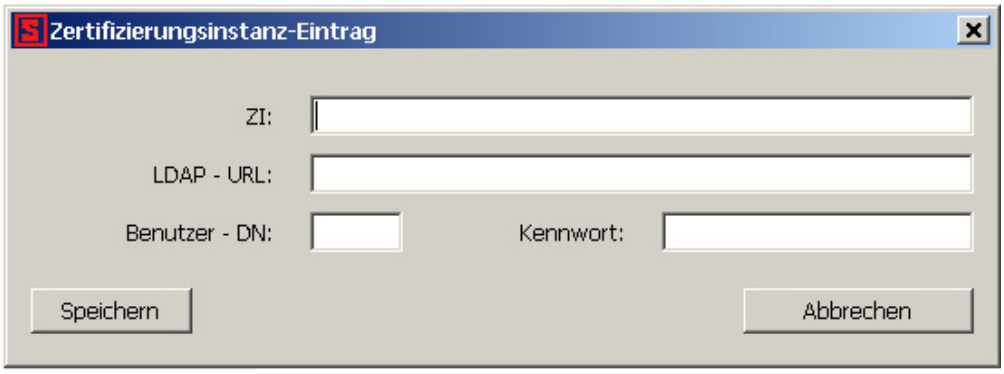


Figure 72: Zertifizierungsinstanz hinzufügen

10.1.2. Daten einer Zertifizierungsinstanz ändern

Um die Daten einer vorhandenen Zertifizierungsinstanz zu ändern, markiert man zuerst den zu ändernden Datensatz. Durch betätigen des Button "Ändern" (oder durch einen Doppelklick auf dem Eintrag) wird der Eintrag editierbar angezeigt (Der Name der Zertifizierungsinstanz kann auf direktem Wege nicht verändert werden. Eine Änderung des Namens der Zertifizierungsinstanz kann dennoch durch Löschen und neu Anlegen derselben erreicht werden):

Figure 73: Zertifizierungsinstanz ändern

10.1.3. Zertifizierungsinstanz löschen

Um eine vorhandene Zertifizierungsinstanz zu löschen, markiert man zuerst den zu löschenden Datensatz. Nun klickt man auf den Button "Löschen" und es erscheint eine Sicherheitsabfrage die zu bestätigen ist:

Figure 74: Zertifizierungsinstanz löschen

10.2. Zertifikatsverwaltung

Zertifikate sind Datenstrukturen, welche bestimmte Informationen wie digitale Schlüssel oder Daten über die ausstellende Zertifizierungsinstanz beinhalten. Zertifikate sind zur Erstellung von digitalen Signaturen zwingend erforderlich. Qualifizierte Zertifikate, welche zur Erstellung von qualifizierten digitalen Signaturen verwendet werden müssen, dürfen ausschließlich von akkreditierten Zertifizierungsinstanzen ausgegeben werden. Als vertrauenswürdige Zertifikate bezeichnet man Zertifikate, welche vom Benutzer als solche definiert werden. Dies bedeutet, der Benutzer muss Aufgrund verschiedener Kriterien, wie beispielsweise der Herkunft eines Zertifikats, entscheiden, ob er das Zertifikat als vertrauenswürdig einstuft oder nicht.

10.2.1. Übersicht

Das **hotSign** –Menü mittels Rechtsklick auf das Systray–Icon öffnen, danach auf „Verwaltung“ - Vertrauenswürdige Zertifikate" klicken.

hotSign bietet verschiedene Funktionen zur Verwaltung von vertrauenswürdigen Stammzertifikaten an. In der Übersicht werden alle importierten Zertifikate in Listenform angezeigt - die Anzeige beinhaltet Information über:

- Seriennummer des Zertifikats
- Antragsteller
- Aussteller des Zertifikats (ZI - Zertifizierungsinstanz)
- Beginn und Ende der Gültigkeitsdauer des Zertifikats.

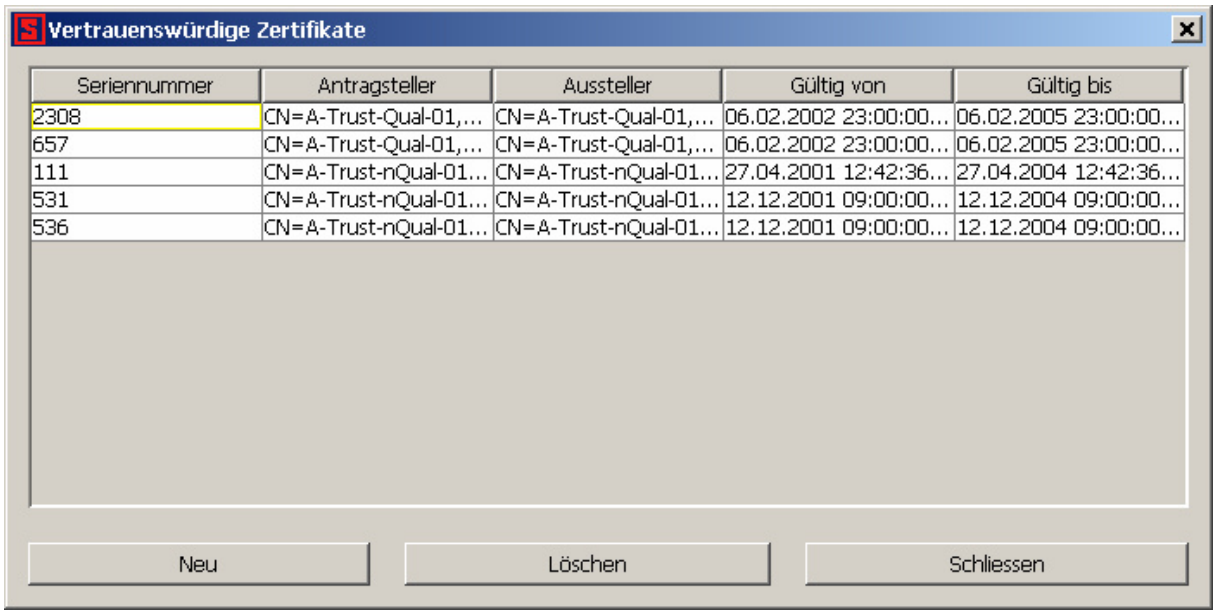


Figure 75: Vertrauenswürdige Zertifikate - Übersicht

10.2.2. Hinzufügen eines Zertifikats

Um ein neues Zertifikat hinzuzufügen, klickt man auf den Button "Neu". Es erscheint nun ein Dateiauswahlmenü, in welchem zu der gewünschten Zertifikatsdatei navigiert werden kann. Der Vorgang kann durch drücken des "Abbrechen"-Buttons beendet werden. Ein Zertifikat wird hinzugefügt, indem man es markiert und anschließend den "Öffnen"-Button anklickt:

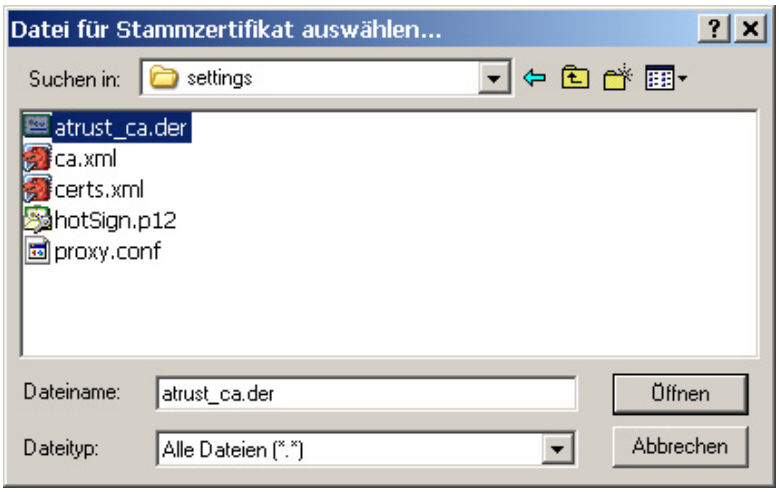


Figure 76: Vertrauenswürdige Zertifikate hinzufügen

Der nun folgende Dialog zeigt den Fingerabdruck (Fingerprint) des Zertifikats, dieser ist mit dem vom Aussteller erhaltenen Fingerabdruck zu vergleichen. Stimmen beide überein, so kann die Sicherheitsabfrage durch Klick auf den "Ja"–Button beendet und das Zertifikat hinzugefügt werden. Stimmt der Fingerabdruck des Zertifikats nicht mit den Angaben des Ausstellers überein, so muss die Sicherheitsabfrage mit "Nein" beantwortet werden. In diesem Fall wird das Zertifikat nicht hinzugefügt.

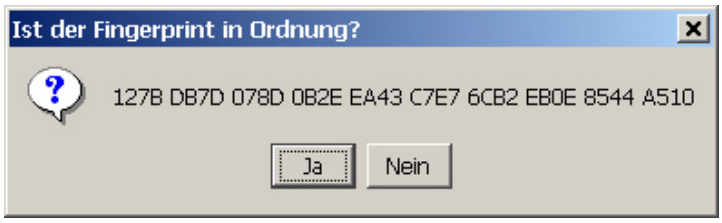


Figure 77: Vertrauenswürdige Zertifikate hinzufügen – Kontrolle Fingerprint

10.2.3. Löschen eines Zertifikats

Um ein Zertifikat zu löschen, markiert man das betreffende Zertifikat durch eine Klick auf die entsprechende Datenzeile, anschließend betätigt man den Button "Löschen". Es erscheint nun eine Sicherheitsabfrage:

Figure 78: Vertrauenswürdige Zertifikate löschen – Sicherheitsabfrage

10.3. Proxy-Einstellungen

Bei der Kommunikation von **hotSign** mit externen Services besteht die Möglichkeit, verschiedene Proxy–Server anzugeben. Dies kann zum Beispiel notwendig sein, wenn mit Hilfe von **hotSign** erstellte Signaturen an einen externen (Web-)Server gesendet werden, und die Kommunikation nur über einen HTTP-Proxy-Server möglich ist

Die Einblendung des Konfigurationsfensters für die Proxy–Einstellungen erfolgt mittels Rechtsklick auf das Systray–Icon und anschließendem Klicken auf „Verwaltung - Proxy-Einstellungen".

Jeweils für einen HTTP-Proxy und/oder SSL–Proxy ist die Möglichkeit eines Eintrages gegeben. Falls eine Authentifizierung am entsprechenden Proxy–Server erforderlich ist, kann diese gesondert eingegeben werden.

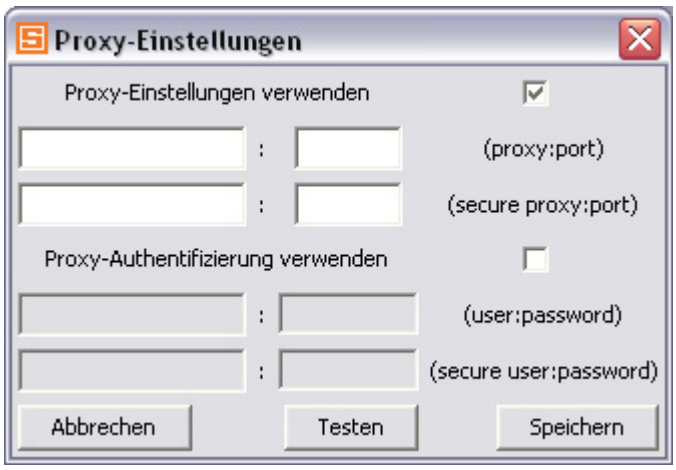
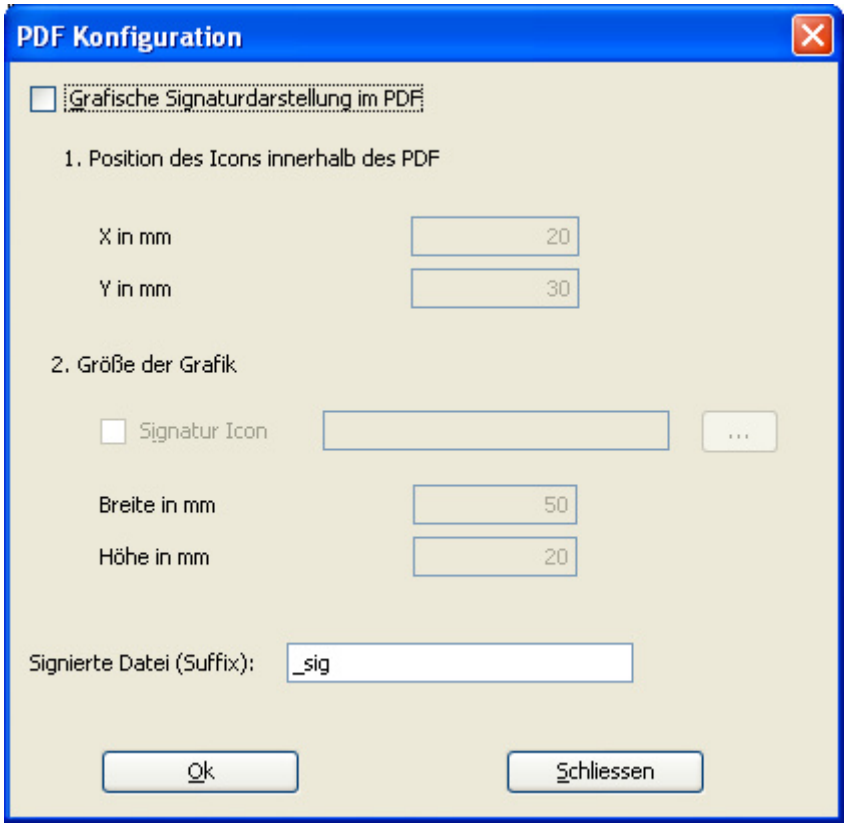


Figure 79: Proxy–Server-Einstellungen vornehmen

Geänderte Einstellungen werden erste bei einem Neustart von hotSign wirksam.

10.4. PDF Konfiguration

Dieses Dialogfenster legt die Einstellungen für PDF-Signaturfelder fest. Dies ist relevant falls hotSign verwendet wird um PDF-Dokumente zu signieren.
Hinweis: Zur Signatur von PDF-Dokumenten muss das PDF-Modul aktiviert werden. Den erforderlichen Aktivierungscode erhalten Sie über den Online-Shop von BDC. Die Aktivierung können Sie in der Folge folgendermaßen vornehmen: siehe 10.5 hotSign Aktivierung



Die Option „Grafische Signaturdarstellung im PDF“ legt fest ob eine „sichtbare“ oder „unsichtbare“ Signatur erstellt werden soll. Ist diese Option deaktiviert enthält das PDF-Dokument nach der Signaturerstellung keine optische Präsentation der Signatur. Falls die Option aktiviert ist, wird in die erste Seite des PDF-Dokuments, an der angegebenen Position (X, Y) ein Signaturfeld eingetragen. Ist zusätzlich die Option „Signatur Icon“ aktiviert und eine Grafik-Datei ausgewählt wird diese in das Signaturfeld – unter Berücksichtigung der angegeben Größe (Breite, Höhe) – eingetragen.

„Signierte Datei (Suffix)“ legt einen Zusatz für Dateinamen fest, mit dem die Dateinamen signierter PDF-Dokumente standardmäßig versehen werden.

10.5. hotSign Aktivierung

Klicken Sie dazu mittels Rechtsklick auf das Systray–Icon von **hotSign** und anschließend auf „Aktivieren“:

In das Feld „Aktivierungscode“ muss der Code eingetragen werden, den Sie von BDC erhalten haben. Die Felder Nachname, Vorname und E-Mail sind MUSS-Felder. Klicken Sie im Anschluss auf „Aktivieren“ um die Aktivierung durchzuführen. In diesem Zusammenhang wird eine Online-Anfrage an den Lizenzierungsserver von BDC gestartet. Die Internet-Verbindung muss daher zur Ausführung dieses Vorgangs aktiviert sein. Falls der Verbindungsaufbau über einen Proxy-Server vorgenommen wird, muss dieser zuvor in hotSign konfiguriert werden (siehe 10.3 Proxy-Einstellungen).
Bei erfolgreicher Aktivierung wird der Text „hotSign ist aktiviert“ angezeigt. Zusätzlich werden die aktivierten Module (zB: eCard, PDF) aufgelistet.

10.6. Weitere Funktionen

10.6.1. Protokoll aufzeichnen

Um allfällig auftretende Fehler lokalisieren zu können, kann eine Protokollfunktion aktiviert werden. Die Aktivierung/Deaktivierung der Protokollfunktion erfolgt mittels „Verwaltung - Protokoll aktiv". Sobald die Funktion „Protokoll aktiv“ aktiviert ist, schreibt **hotSign** ein Log über durchgeführte Programmaktionen mit (welche zur Fehlerfindung sehr hilfreich sein können). Die Protokoll–Einträge werden in die Datei „java.log“, die sich im Windows–System-Verzeichnis befindet, geschrieben.

10.6.2. Autoupdate

Beim Starten von **hotSign** wird eine verschlüsselte Verbindung zum Update – Server aufgebaut, um eventuell vorhandene Updates automatisch zu installieren. Die Deaktivierung/Aktivierung dieser Funktion erfolgt mittels „Verwaltung – Autoupdate beim Programmstart"

10.6.3. Tip des Tages

Beim Starten von **hotSign** wird automatisch ein „Tip des Tages angezeigt“. Die Deaktivierung/Aktivierung dieser Funktion erfolgt mittels „Verwaltung - Tip des Tages"

10.6.4. Standard Infobox-PIN verwenden

Die a.sign Premium Signaturkarte wird standardmäßig mit der Infobox-PIN „0000“ ausgeliefert. Sofern diese vom Karteninhaber nicht geändert wurde, kann diese Option aktiviert werden. Beim Auslesen der Personenbindung (beispielsweise im Rahmen von Portal-Logins mittels Signaturkarte) erspart sich der Karteninhaber die Eingabe der Infobox-PIN.

10.6.5. Über BDC "hotSign"

Informationen über die **hotSign** -Programmversion können wie folgt erhalten werden:
hotSign –Menü mittels Rechtsklick auf das Systray–Icon öffnen, anschließend auf „Über BDC hotSign" klicken. In diesem Dialogfenster wird zusätzlich angezeigt welche hotSign-Module aktiviert sind. Folgende Module stehen zur Verfügung:

- E-Card
- PDF
- D-Trust

11. Barrierefreiheit

hotSign wurde speziell auf diese Anforderung hin optimiert. Grundsätzlich können Screen Reader verwendet werden, die die Java Accessiblity Bridge unterstützen. Diese muss zunächst geladen und installiert werden. Sie erhalten diese im Download-Bereich von SUN: http://java.sun.com/javase/technologies/accessibility/accessbridge/index.jsp.
Wir empfehlen als Screen Reader die Software „JAWS“ zu verwenden.

12. Häufige Fehlerursachen

Kein erkanntes Kartenlesegerät
Seit der Ausführung des **hotSign**-Setups wurde möglicherweise ein anderer Kartenleser installiert (oder nachträglich für eine andere Schnittstelle konfiguriert). Durch erneutes Ausführen des Setups kann ein neuer Leser/Port ausgewählt werden (siehe Punkt 7.3 Änderung von Kartenlesegerät und/oder Port).

PIN ungültig
Im **hotSign** Secure-Viewer ist auf der obersten Titelleiste angegeben, welche PIN (Signatur-PIN oder Geheimhaltungs-PIN) bei der Signaturerstellung zu verwenden ist. Die Signatur-PIN ist 6-stellig - die Geheimhaltungs-PIN 4-stellig. Je nach verwendeter Signaturkarte besteht nur eine gewisse Anzahl an Versuchsmöglichkeiten!

PIN-Eingabe bei Verwendung eines Cherry Smartboards
Die Möglichkeit der PIN-Eingabe besteht ab dem Zeitpunkt des rot blinkenden PIN-Symbols auf der Tastatur. Eventuell wird jedoch der entsprechende PIN-Eingabe-Auffforderungsdialog schon etwas früher angezeigt.

PIN wird zu langsam eingegeben
Die Zeitspanne für die Eingabe einer PIN am Kartenlesegerät ist aus Sicherheitsgründen begrenzt. Wenn diese Zeitspanne verstreicht wird die Signaturerstellung abgebrochen.

Ein hotSign Fenster ist verschwunden
Es handelt sich bei **hotSign** um eine Applikation, die im Wesentlichen in der Programmiersprache Java geschrieben wurde. Dies führt dazu, dass **hotSign** nicht in der Taskleiste aufscheint. Um dennoch zu einem **hotSign** –Fenster zu wechseln, kann der Benutzer die „Alt“–Taste gedrückt halten und sich anhand der Tabulator–Taste „Tab“ durch die laufenden Prozesse bewegen.

Unerwarteter Fehler
Das Auftreten dieses Fehlers könnte ein Hinweis darauf sein, dass die Installation von hotSign zerstört oder beschädigt wurde. Ein erneutes Installieren von hotSign sollte dieses Problem beheben.

13. hotSign FAQ

13.1. Installation

Q: *Was bewirkt die Integritätsprüfung von **hotSign**?*
A: Die von **hotSign** verwendeten Programmteile werden zur Laufzeit vor eventuellen Angriffen geschützt.

Q: *Kann ich **hotSign** installieren, wenn ich keine Kartenlesertreiber installiert habe?*
A: Ja, die Installation von **hotSign** ist auch möglich, wenn keine Kartenleser installiert wurden. In diesem Fall wird **hotSign** installiert, es können jedoch keine Signaturen erstellt werden. Um Signaturen erzeugen zu können, muss ein Kartenleser installiert und angeschlossen werden und anschließend das **hotSign**-Setup erneut ausgeführt und der betreffende Kartenleser konfiguriert werden.

Q: *Kann ich **hotSign** installieren, wenn ich den Kartenleser nicht angeschlossen habe?*
A: Ja, die Installation von **hotSign** ist auch möglich, wenn keine Kartenleser angeschlossen wurden. In diesem Fall wird **hotSign** installiert, es können jedoch keine Signaturen erstellt werden. Um Signaturen erzeugen zu können, muss ein Kartenleser installiert und angeschlossen werden und anschließend das **hotSign**-Setup erneut ausgeführt und der betreffende Kartenleser konfiguriert werden.

Q: *Ich habe den Kartenleser angeschlossen und die Treiber installiert, das Setup findet den Kartenleser jedoch trotzdem nicht. Was kann ich tun?*
A: Starten Sie ihren Rechner neu. Hilft diese Maßnahme auch nicht, installieren Sie den Kartenlesertreiber neu.

13.2. Betrieb

Q: *Wozu werden die Informationen zu den Zertifizierungsinstanzen benötigt? Kann ich diese löschen?*
A: Um die Gültigkeit eines Zertifikates (und somit einer Signatur) prüfen zu können, muss eine Verbindung zu einer Zertifizierungsinstanz über LDAP aufgebaut werden. Somit muss für das zu verwendende Zertifikat die zugehörige Zertifizierungsinstanz eingetragen sein. Wird diese Information gelöscht, kann die Gültigkeit des Zertifikates nicht überprüft werden.

Q: *Warum müssen die vertrauenswürdigen Zertifikate lokal vorhanden sein?*
A: Bei der Zertifikatsprüfung ist das Zertifikat selbst über ein anderes Zertifikat signiert, somit ist seine Echtheit sichergestellt. Dieses Signaturzertifikat ist wiederum mit einem Zertifikat signiert, usw... Dies geht bis zu dem sogenannten Wurzelzertifikat, welches selbstsigniert ist und somit als vertrauenswürdig einzustufen ist. Damit diese nicht gefälscht werden können, müssen sie lokal vorhanden sein, um eine gültige Prüfung der Zertifikate zu gewährleisten.

Q: *Welches Format müssen Zertifikate haben, um importiert werden zu können?*
A: Vertrauenswürdige Zertifikate werden aus einer Datei importiert, diese muss DER kodiert vorliegen, das Zertifikat selbst muss dem Standard X509v3 folgen.

Q: *Wenn ich die PIN ändern will, wie lange muss/darf diese sein?*
A: Die Länge der PIN ist abhängig von der verwendeten Signaturkarte. Meist ist eine Mindestlänge von 6 Zeichen einzuhalten, die Maximallänge kann variieren.

Q: *Wie finde ich eventuell benötigte Proxy–Einstellungen für **hotSign** heraus?*
A: Unter Windows finden Sie die Internetoptionen in der Systemsteuerung. Dort klicken Sie auf den Reiter “Verbindungen”, dort auf den Button “Einstellungen”. Hier finden Sie die Angaben

zu den Proxy–Einstellungen des Systems. Sind diese Einstellungen nicht korrekt, wenden Sie sich an ihren Netzwerkadministrator bzw. an ihren Internetanbieter.

Q: *Über das Kontextmenü (rechte Maustaste auf das **hotSign** Icon) wurde die Protokollierung aktiviert. Wie kann ich das Protokoll einsehen?*
A: Die Protokolldatei befindet sich in ihrem Systemordner (z.B. unter "C:\windows\system32"). Die Datei heißt "java.log" und ist mit einem Texteditor einsehbar (zum Beispiel NotePad).

Q: *Woher weiß ich, welche PIN ich zur Signatur eingeben muss?*
A: Diese Information entnehmen Sie der Titelleiste des **hotSign** –Secure-Viewers.

Q: Wie kann ich die Online–Hilfe einsehen?
A: Durch drücken der F1–Taste bei den entsprechenden Konfigurationsmasken bzw. Secure-Viewer von **hotSign**.

Q: *Was bedeutet die Meldung "Die Zertifikatskette konnte nicht aufgelöst werden"?*
A: Ein Zertifikat ist immer Teil einer Kette (ausgenommen es ist selbstsigniert). Um die Gültigkeit und vor allem die Echtheit des Zertifikates zu gewährleisten, wird dieses mit einem Zertifikat signiert, dass in der Kette eine Stufe über dem Signaturzertifikat liegt. Dieses Zertifikat ist wieder signiert, usw.. Konnte ein oder mehrere Zertifikat(e) dieser Kette nicht geladen werden, so kann diese Kette nicht geprüft (oder aufgelöst) werden. Meist liegt dies an der LDAP Verbindung zu den Zertifikatsinstanzen.

14. Glossar

Bürgerkarte — *Die Bürgerkarte ist ein "amtliche Ausweisdokument" im elektronischen Verwaltungsverfahren, etwa im Behördengang über das Internet*

Bürgerkartenumgebung — *Software die über das Kartenlesegerät mit der Signaturkarte kommuniziert und die erforderliche Bürgerkartenfunktionalität zur Verfügung stellt.*

Fingerprint — *Der Fingerprint eines Zertifikates ist der Hashwert dieses Zertifikates. Durch diesen Hashwert kann die Authentizität des Zertifikates überprüft werden.*

Infoboxen — *Infoboxen sind Datenspeicher die im Konzept Bürgerkarte vorgesehen sind.*

LDAP — *Lightweight Directory Access Protocol – ein Verzeichnisdienst im Internet*

Personenbindung — *Eine von der Stammzahlenregisterbehörde signierte Struktur, welche ein eindeutiges Identifikationsmerkmal einer Person einem oder mehreren Zertifikaten dieser Person zuordnet*

PIN — *Personal Identification Number*

PKI — *Public Key Infrastruktur*

Proxy–Server — *Eine Proxy-Server ruft auf Anforderung Dokumente von einem Server ab und übergibt sie an einen Client. Der Vorteil eines Proxy-Servers liegt darin, dass Dokumente normalerweise zwischengespeichert werden.*

PUK — *PIN Unblocking Key*

Secure–Viewer — *Für die Signaturerstellung verwendete Software die es dem Signator ermöglicht, sich das zu signierende Dokument sicher anzusehen und dann den Signaturvorgang auszulösen.*

Bürgerkarte	*Die Bürgerkarte ist ein "amtliche Ausweisdokument" im elektronischen Verwaltungsverfahren, etwa im Behördengang über das Internet*
Security-Layer-Protokoll	*Jene Schnittstelle, über die eine Applikation auf Funktionen der Bürgerkarte zugreift, um beispielsweise eine elektronische Signatur zu erstellen oder vom Datenspeicher der Bürgerkarten-Umgebung zu lesen.*
Signatur	*Ergebnis der asymmetrischen Verschlüsselung einer Nachricht (oder des Hashwerts einer Nachricht) mit einem privaten Schlüssel. Da sich die Nachricht (oder der Hashwert) nur mit dem zugehörigen öffentlichen Schlüssel entziffern lässt, darf man annehmen, dass die elektronische Signatur vom Schlüsselinhaber erstellt worden ist.*
Signaturschlüssel	*Bei einem Public-Key-Verfahren: der geheime und der dazugehörige öffentliche Schlüssel.*
Signaturkarte	*Auf einer Signaturkarte (Chipkarte) werden die private Schlüssel und die entsprechenden Zertifikate sicher abgelegt, so dass Nachrichten elektronisch signiert und entschlüsselt werden kann.*
XHTML	*eXtensible Hypertext Markup Language - Auszeichnungssprache für das World Wide Web*
XML	*eXtensible Markup Language - Eine Sprache, mit der sich Auszeichnungssprachen definieren lassen.*
Zertifikat	*Digitale Zertifikate sind das elektronische Gegenstück zu einem Ausweis. Sie ordnen ihrem Inhaber eindeutig einen öffentlichen Schlüssel (Public Key) und damit einer digitalen Signatur zu, die nur mit dem korrespondierenden privaten Schlüssel erzeugt worden ist.*
Zertifizierungsinstanz	*(Auch Certificate Authority oder Trustcenter) Natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen.*

15. Benutzte Bibliotheken

Der BDC **hotSign** Signatur–Client benutzt folgende Bibliotheken:

- Embedded Integrity Services Library der CDSA Version 2.0, © The Open Group, 2000
- Virtual X Class Library, © The VXCL Alliance, 1996-2000
- OpenSSL Toolkit, © The OpenSSL Project, 1998-2000, © Eric A. Young, Tim J. Hudson, 1995-1998
- Apache Xerces. Entwickelt von der Apache Software Foundation.
- Apache Xalan – XSLT processer. Entwickelt von der Apache Software Foundation

16. Lizenzen

16.1. CDSA

Intel Open Source License for CDSA/CSSM Implementation
(BSD License with Export Notice)

Copyright (c) 1996-2001 Intel Corporation
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions

are met:

+ Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

+ Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

+ Neither the name of the Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

EXPORT LAWS: THIS LICENSE ADDS NO RESTRICTIONS TO THE EXPORT LAWS OF YOUR JURISDICTION. It is licensee's responsibility to comply with any export regulations applicable in licensee's jurisdiction.
This software is subject to the U.S. Export Administration Regulations and other U.S. law, and may not be exported or re-exported to certain countries (currently Afghanistan (Taliban-controlled areas), Cuba, Iran, Iraq, Libya, North Korea, Serbia (except Kosovo), Sudan and Syria) or to persons or entities prohibited from receiving U.S. exports (including Denied Parties, Specially Designated Nationals, and entities on the Bureau of Export Administration Entity List or involved with missile technology or nuclear, chemical or biological weapons).

Copyright (c) 1996-2001 Intel Corporation. All rights reserved.
* Other brands and names are the property of their respective owners.

16.2. VXCL

VXCL - The Virtual X Class Library.
Copyright (C) 1996-2001 The VXCL Alliance.

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

Primary Author of this source code file: Todd Osborne (todd@vxcl.org)
Other Author(s) of this source code file:

EXCEPTION NOTICE (Borrowed partly from the wxWindows Class
Library license (http://www.wxwindows.org) exception provided by
Julian Smart (julian.smart@ukonline.co.uk) and others:

1. As a special exception, the copyright holders of this library give permission for additional uses of the text contained in this release of the library. The exception is that you may use, copy, link, modify and distribute under the user's own terms, binary object code versions of works based on the Library.

2. If you copy code from files distributed under the terms of the GNU General Public License or the GNU Library General Public License into a copy of this library, as this license permits, the exception does not apply to the code that you add in this way. To avoid misleading anyone as to the status of such modified files, you must delete this exception notice from such code and/or adjust the licensing conditions notice accordingly.

3. If you write modifications of your own for this library, it is your choice whether to permit this exception to apply to your modifications. If you do not wish that, you must delete the exception notice from such code and/or adjust the licensing conditions notice accordingly.

16.3. OpenSSL

LICENSE ISSUES
==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.

OpenSSL License

```
/* ====================================================================
 * Copyright (c) 1998-2005 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
```

*
*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the rouines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or

```
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```

16.4. Apache Software Foundation

```
/*
 * The Apache Software License, Version 1.1
 *
 *
 * Copyright (c) 1999 The Apache Software Foundation.  All rights
 * reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. The end-user documentation included with the redistribution,
 *    if any, must include the following acknowledgment:
 *       "This product includes software developed by the
 *        Apache Software Foundation (http://www.apache.org/)."
 *    Alternately, this acknowledgment may appear in the software itself,
 *    if and wherever such third-party acknowledgments normally appear.
 *
 * 4. The names "Xerces" and "Apache Software Foundation" must
 *    not be used to endorse or promote products derived from this
 *    software without prior written permission. For written
 *    permission, please contact apache@apache.org.
 *
 * 5. Products derived from this software may not be called "Apache",
 *    nor may "Apache" appear in their name, without prior written
 *    permission of the Apache Software Foundation.
 *
 * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
 * DISCLAIMED.  IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
 * LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
 * USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
 * ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
 * OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
 * OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 * ====================================================================
 *
 * This software consists of voluntary contributions made by many
 * individuals on behalf of the Apache Software Foundation and was
```

```
* originally based on software copyright (c) 1999, International
* Business Machines, Inc., http://www.ibm.com.  For more
* information on the Apache Software Foundation, please see
* . */
```